



THE DARK OVERLORD

CYBER INVESTIGATION REPORT



NIGHT LION
SECURITY

V1.01

TABLE OF CONTENTS

1.0

INTRODUCTION

1.1	Executive Summary	4
1.2	TDO Victimology	5
1.3	Other Breach Victims	6
1.4	Forums and Markets Index	7
1.5	Stylometry Analysis	8
1.6	Data Viper	9

2.0

HISTORY & OPERATING PROCEDURES

2.1	Group Structure	11
2.2	Modus Operandi	12
2.3	Communication and Personality	12
2.4	Group Structure	15
2.5	Use of Media	16
2.6	Group Formation	17
2.7	TDO's First Appearances	19
2.8	Initial Members	20
2.9	De-Evolution of the Group	22
2.10	Communicating with TDO	23
2.11	TDO appears on KickAss	24
2.12	The End of The Dark Overlord	25
2.12	Post-Mortem	26

3.0

BREACH STATISTICS

3.1	Results Summary	28
3.2	Data Analysis	29

4.0

ACTOR PROFILES 27

4.1	Threat Actor Matrix	28
4.2	Cr00k	29
4.3	Peace of Mind	42
4.4	Arnie	59

5.0

AFFILIATIONS

4.1	NSFW	68
4.2	Gnostic Players	69
4.3	Shiny Hunters	71
4.4	Connecting The Pieces	72

A

APPENDIX

5.1	Timeline Summary	77
5.2	A Late Night Convo with TDO	78
5.3	Hunting Cyber Criminals	80
5.4	Breach Lists	81



Section 1

The Dark Overlord

Introduction

EXECUTIVE SUMMARY

In 2016, a hacking group known as 'The Dark Overlord' (TDO) began terrorizing and extorting organizations. The group quickly became known throughout the media for its extortion of medical providers and the sale stolen medical records. Some of the group's first publicized hacks include medical facilities and law firms in Missouri.

In 2017, the group gained additional headlines for extorting companies like Disney and Netflix, threatening to release advanced copies of their studio productions if their ransom demands were not met.

Later that year TDO moved from traditional hacking and extortion schemes to terror-based attacks, when they targeted school districts, and directly threatened the lives of students if their demands were not met. This act forced the closure of more than 30 schools for an entire week.

On January 01, 2017, TDO announced a "change of ownership" over Twitter. We believe two of the three actors described in this report ceased working with the group around this time. Following this announcement, all actions taken as part of The Dark Overlord can be traced back to one key individual: Christopher Meunier of Calgary, Canada.

This report will also provide context into two additional threat actors, Dionysios "Dennis" Karvouniaris, of Calgary, Canada, and Nathan Wyatt, of U.K., England, believed to be a part of the group in 2016.

This report will also provide evidence of ongoing criminal collaboration between Meunier and his childhood friend, Mr. Karvouniaris, under the group names ROR[RG], NSFW, Gnostic Players, and Shiny Hunters.

The collaboration of these two individuals can be directly attributed to roughly 42% of all non-credit card related data breaches that occurred between January 2017 to June of 2020.

Finally, this report will directly link the boys in a recent hack of our servers, designed to discredit the findings of this report.

1.2

THE DARK OVERLORD VICTIMOLOGY

The following list of organizations have been publicly extorted by The Dark Overlord.
This list only includes organizations that have been made public.

A.M. Pinard et Fils, Inc.	Holland Eye Surgery and	OG Gastrocare
ABC Studios (Steve Harvey)	Laser Center	PcWorks, L.L.C
Adult Internal Medicine of N. Scottsdale	INdigofera Jeans	Peachtree Orthopedic Clinic
Aesthetic Dentistry	International Textiles & Apparel - Los Angeles, CA	Photo-Verdaine
American Technical Services	Johnston Community School District	PilotFish Technology (PFT)
Athens Orthopedic Clinic	La Parfumerie Europe	Pre-Con Products
Auburn Eyecare	La Quinta Center for Cosmetic Dentistry	Prosthetic & Orthotic Care
Austin Manual Therapy	Larson Studios / Netflix	Purity Bakery Bahamas
CB Tax Service	Line 204	Quest Records, LLC
Coliseum Pediatric Dentistry	Little Red Door Cancer Services of East Central Indiana	Royal Bank of Canada
Dougherty Laser Vision	London Bridge Plastic Surgery	School District 6 - Colombia Falls, MT
DRI Title	Marco Zenner	Select Pain & Spine
Family Support Center	Menlo Park Dental	SMART Physical Therapy
Feinstein & Roe	Mercy Healthcare	St. Francis Health System
Flathead Falls School District	Midwest Imaging Center	Tampa Bay Surgery Center
G.S. Polymers	Midwest Orthopedic Clinic	UniQoptics, L.L.C
Gorilla Glue	Mineral Area Pain Center	Unnamed Victim (NY)
H-E Parts Morgan		Van Ness Orthopedic and Sports Medicine
Hand Rehabilitation Specialists - Vermont		WestPark Capital
Hiscox (Hoax)		

1.3

OTHER BREACH VICTIMS

The following victims can be linked to the primary threat actors discussed in this report.

Additional aliases used include:

ROR[RG]

NSFW

Gnostic Players

Shiny Hunters

8tracks	Flipboard	Quora
Accuradio.com	Foodera	RedBull Sound Select
Adult Friend Finder	FrontLineSMS	Sephora
Army Force Online	GSMA Intelligence	Startribune
AT&T (3rd party partner)	Lead 411	StockX
Bell Canada	Leafly	Talend
BotOfLegends	LifeSafer / LMG Holdings	Taringa
Carding Mafia	Linux Mint	TeamSkeet
Catho	LivSpace	Timehop
Chegg	Massachusetts Institute of	Tokopedia
Chronicle.com	Technology (MIT)	Turkish National Police
CodeChef	Mathway	Unacademy
Datalot	MGM Grand International	University of Phoenix
Door Dash	Minted	Voxy
DotaHut	MPGH	Voxy
DrawMyThing.com	MyHeritage	Wappalyzer
Elections.ca	Omlette.com.br	Wego
FemaleDaily	PiZap	Wishbone
Filmow	PolyCount	Zoomcar
FiveStars	Poshmark	Zoosk

(Complete list of Gnostic Players victims omitted from this list)

1.4

FORUMS AND MARKETS GLOSSARY

BLACKBOX (BB)

Private hacking forum run by Ghost (aka Cyper), following the demise of Hell Forum.

EXPLOIT

Active russian hacking forum.

HELL FORUM (HF)

Darknet Hacker forum run by 'Ping'. Hell Forum closed in 2016 following Ping's "arrest".

HELL RELOADED (HR)

Hell Reloaded was the second version of Hell Forum, launched following the collapse of the original forum.

KICK-ASS (KA)

Kick-Ass is an English-speaking darknet hacking forum, run by user NSA (aka Cyper).

SIPHON

Former darkweb hacking forum. The present clearnet site offers public exploits and data dumps.

THE REAL DEAL (TRD)

Darknet marketplace specializing in selling hacked data and code exploits. Used as the main sales hub for the sale of TDO data.

XDEDIC MARKETPLACE (XD)

Online marketplace where users can purchase RDP access to servers from around the world.

STYLOMETRY ANALYSIS

In August 2018, Professors Rachel Greenstadt and Aylin Caliskan presented a talk at DEFCON 26 on “De-anonymizing Programmers from Source Code and Binaries”.¹ The talk was designed to show how machine learning could be used to de-anonymize programmers by identifying “stylistic fingerprints” within code samples.

As described in an article by Wired Magazine, Caliskan, Greenstadt, and two other researchers demonstrated that even small snippets of code on the repository site GitHub can be enough to differentiate one coder from another with a high degree of accuracy.²

Rachel Greenstadt and Bander Alsulami were kind enough to assist in this investigation by offering to test a number of code samples related to the threat actors in this research and compare them against fully attributed code samples.

The results will be discussed in subsequent sections of this research as they pertain to each threat actor.

JGAAP

We would also like to extend a special thank you for the assistance of Evllabs (www.evllabs.com) and Sean Vinsick for their support with the Java Graphical Authorship Attribution Program (JGAAP).

JGAAP is an open-source stylometry analysis tool. The results derived from the stylometry analysis of various actor's forum posts was enough to help identify additional aliases in several TDO members.

JGAAP can be downloaded at <https://github.com/evllabs/JGAAP>.

¹ <https://www.defcon.org/html/defcon-26/dc-26-speakers.html#Greenstadt>

² <https://blog.wired.com/story/machine-learning-identify-anonymous-code/>

1.6



Data Viper (www.dataviper.io) is a threat intelligence platform specifically developed to help identify the members of The Dark Overlord.

The tool was designed to identify key pieces of the group's origins and help trace their current whereabouts. As part of our official investigation, a number of other threat intelligence firms were contacted for assistance. No single organization or tool possessed the necessary data to form a complete picture of the threat actors, so we developed our own tool.

Data Viper is the culmination of almost two years' worth of effort, in not only developing the platform, but in cultivating the black-market relationships needed to acquire the historical data necessary to fuel the tool and ultimately identify these criminals.

The evidence provided in this report originated from data breaches, paste scrapes, and historical darknet forum data, all of which have been indexed and are now available as part of the big-data threat intelligence and analytics tool known as Data Viper.

The tool is now available for all organizations wanting real-time actionable intelligence to help protect themselves, and to investigative teams and law enforcement agencies wanting adversarial threat intelligence.

For more information, visit www.dataviper.io



Section 2

The Dark Overlord

History & Operating Procedures

OVERVIEW

BEGININGS

TDO made their first public appearances in 2016, when members of the group gained access to several medical facilities and began releasing personal client records in order to increase the value of their extortion demands. Evidence suggests that the group initially gained RDP (remote desktop protocol) access to their first medical clinic by purchasing the compromised access from Xdedic, a dark web marketplace.

From there, the group identified a vulnerability within medical software that allowed them to gain access to additional medical victims. The victims ranged in size, and were often asked to pay excessive amounts of money in exchange for not having their confidential documents published on the internet.

GROUP STRUCTURE

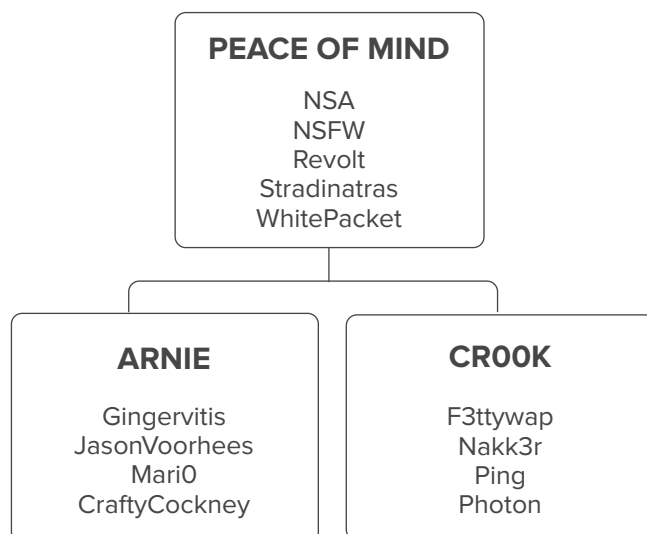
The Dark Overlord group consisted of four core members and a small network of contractors used to carry out menial tasks.

Evidence suggests The Dark Overlord group was formed circa 2015. The group's origins can be traced back to Hell, a dark web hacking forum.

In 2016, the group's assumed leader was Arnie. This was by design, intended to shift focus away from other group members towards the group's assumed leader. "Arnie" was nothing more than a patsy account used to post information on new victims and coordinate sales.

The group's real leaders always remained behind the scenes. This structure is repeated today with the group Shiny Hunters.

In 2017, TDO publicly announced a change in leadership over Twitter, marketing the end of the "Arnie" persona (TDO1), and the beginning of The Dark Overlord persona (TDO2).



@tdohack3r

you know i am not alone?
i have team
we have aexpert english speaker for ransom
i do hacks
others steal the data
i am good at exploit and attack
partner is good at english and business
another is good at stealing data ad running backup and server
making ransomware

2.2

MODUS OPERANDI

RDP ACCESS AS AN INITIAL ATTACK VECTOR

A majority of TDO's initial victims were the result of access through unsecured RDP (remote desktop protocol)*. It is believed that access to the victim's servers was purchased through XDedic,³ as installations of XDedic's custom software tools have been discovered on a number of TDO's victim's servers.⁴ Once inside, TDO would pillage any data and use it to facilitate their ransom demands.

**RDP via Xdedic as the primary attack vector is confirmed in the Arnie section of this report.*

HL7 MEDICAL SOFTWARE

Another possible attack vector initially used by the group was backdoor access to the HL7 Healthcare software. In an interview with DataBreches.net⁵, TDO made the following statement,

"I used their code to find exploits in all their clients.... Also, since I was in their system, I signed a backdoor into their client – because I had access to their certificate signing. It got pushed out in an update a few weeks ago."

INITIAL EXTORTION ATTEMPT

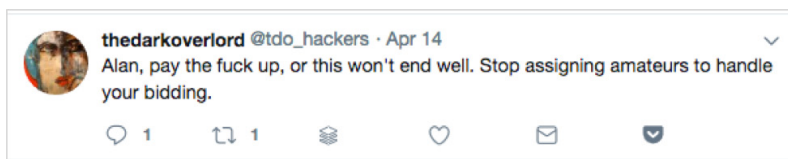
Initial communication of TDO to any victims will occur via email. The group members typically send 2 or 3 messages to various officials within the organization.

If email communication with a victim fails or proves to be unsuccessful, TDO's next attempt to obtain their ransom demands will often come in the form of a public message via Twitter. TDO's twitter accounts include @tdo_hackers, @thedarkoverlord and @tdohack3r.



CONTINUED HARASSMENT

If TDO's initial demands are not met, the tone of their communication and tweets will inevitably become hostile. TDO's impatience will cause them to become frustrated and hostile, often resulting in publicly lashing out at victims. TDO will continue to harass employees of the organization by directly sending them copies of any stolen material.



3 <https://www.kaspersky.com/blog/xdedic-ii/15147/>

4 <https://www.flashpoint-intel.com/blog/cybercrime/xdedic-rdp-targets/>

5 <https://www.databreches.net/hl7-vendor-hack-compromised-clients-ehr-records-the-dark-overlord/>

2.3

COMMUNICATION AND PERSONALITY

SUPERIOR, CONDESCENDING, IMPATIENT

Starting around 2017, any communication with group members became standardized against "The Queen's English" in order to present a unified and structured group. In a direct conversation with one of the group members, it was revealed that all communication was run through a PHP-based translator.

TDO: You fucking Americans have no fucking humour at all, fucking twats.
TDO: A bunch of illiterate wankers.
VT: it would be a section in my book
TDO: You're stoking my ego cock pretty good right now, so go on.
VT: whats up with that 7 page ransom note? wasnt that a bit excessive?
TDO: We are verbose and condescending, quoted by the FBI.
TDO: That's quite literally what they said about our letters.
TDO: 'verbose and condescending'

PERSONALITY

Direct communication with TDO always contains a high level of grandiosity, especially when discussing business, or their "hacking skills". During this researcher's first conversations with TheDarkOverlord on November 2017, TDO took great care in describing his business savvy and often would describe the success of the "brand" they created, and would only refer to themselves as 'we'.

Their general communication style is overly formal, but the actors will quickly become aggressive if their demands are not met or if their ego has been challenged.

CHANGES IN COMMUNICATION

The language style between the original TDO (Arnie, 2016) and TDO2 (2017-2019) is significant, changing from a fake broken accent to overly formal English. Despite the formality, TDO's second leader would come across as impatient and juvenile, often resorting to making criticizing remarks with sexual undertones.

It is our opinion that TDO's initial communications were handled by a spokesperson, possibly Cr00k. TDO later confirmed that he did not know of our previous conversation due to an employee change-over.

The member you spoke with is no longer with us. They mysteriously disappeared and we did not receive the communication logs.

AN INITIAL CONVERSATION WITH THE DARK OVERLORD

Initial conversations with TDO portrayed someone deliberate with their wording, who appeared eager to discuss the workings of their business operation while demonstrating their own superior intelligence.

VT: why is cr00k no longer in the group?

TDO: Is he no longer in the group?

VT: is he still in? It looks like he hasn't posted anything since 2016

TDO: We've contracted a great deal of individuals to front for us as data brokers. It's difficult finding the time to do these things when we're busy climbing out way up the hacking chain.

VT: oh, that's interesting. i guess i never looked at it that way.

VT: ok, so if he is a broker, why is he no longer being used?

TDO: As a business owner, we're surprised you hadn't considered the 'supply chain' methodology and its benefits.

VT: i guess i had no idea how organized the group is.

TDO: Do you believe it's an intelligent decision to allow others to adsorb the disadvantages and costs of stylometry, metadata collection, and other sorts of HUMINT?

VT: absorb them how? in terms of mis-information?

TDO: Risk.

VT: if we are going to discuss a previous broker, it is important to know why they were selected and why they are no longer involved

TDO: We believe our brokers sub-leased much of the work, even. It's difficult for us to acquire an accurate picture of everything.

TDO: Peace, though, how did you come to that one?

VT: because of the w0rm site

TDO: That would make us privy to the likes of some of the planet's largest breaches.

VT: it seems like you guys certainly have the skill.

TDO: Is this something your wife told her school's sports team?

VT: my wife doesn't go to school?

VT: oh. ha ha.

TDO: It's a bit of jest, mate. We're cracking one on you.

2.4

GROUP STRUCTURE

In the following conversation, user c86x (cr00k) discusses the group's structure.

c86x: bruted RDP
c86x: then sell for 100k
c86x: makes no sense
c86x: i can tell you something? he put those prices, not for everyone to buy, but to see
c86x: he is not only in business of selling
c86x: he was blackmailing the owner(s) of clinic
c86x: that's why he went to the news everywhere
c86x: that's why TDO is not on any forum, only on 1 stupid darknet market for journalists
xxx: how do u know so much?
xxx: know tdo and peace were fuckin w people
c86x: i think he mentioned it in an interview
c86x: i know TheDarkOverlord, not with initial TDO sorry
c86x: we deal with criminals, he deals with legit people
...
c86x: yes i forward sales to proter3
c86x: he's the hacker, i'm the seller

INTERNAL TENSIONS & LEADERSHIP CHANGES

User Columbine (believed to be NSA) describes the formation of TDO by NSA and Arnie, as well as internal tensions between the group. Columbine appears to want to deflect all culpability away from NSA.

Columbine: A lot of the other niggers gone too
Columbine: Like NSA@rows.io
Columbine: They formed thedarkoverload
Columbine: that ransoming group
Columbine: I did hear that Arnie was getting mad at NSA though
Columbine: So internal tension between the group
Columbine: NSA barely did shit for TDO I heard
Columbine: and still he got the money
Columbine: so Arnie (who did most of the work) got mad

In 2017, TDO publicly announced a “management change” over Twitter. We believe this marks the change in leadership between Arnie (TDO1) and NSA (TDO2).

2.5

USE OF MEDIA

The Dark Overlord group is known for their use of media to both intimidate their victims and manipulate facts to their advantage. Motherboard published an article in which they state ‘The hacker behind a recent slew of healthcare organization breaches is deliberately using the media to intimidate his victims’.⁶

ORIGINAL MEDIA MANIPULATION

Prior to forming TDO, this report will show how members of the group would use and manipulate the media to serve their needs. Subsequent sections of this report will show how the group originally manipulated a reporter to pin the identity of one of their members on to someone else.

Following the formation of the group, and the evolution of the individual threat actors, the manipulation tactics of TDO continue to involve the media. TDO would often work with a small handful of selected journalists and media outlets to raise awareness of attacks in order to facilitate bigger extortion payments.

DATABREACHES.NET

Over the past several years, TDO has worked directly with databreaches.net owner Dissent Doe. Dissent has written extensively on TDO, covering many of the group's hacks and often providing insight into the group through direct communication with its members.

In one such example, “TDO provided this site with a preview of some of the material, which included XXX: Return of Xanger Cage (2017), Bill Nye Saves The World (Season 1), & Orange Is The New Black (Season 5)”.⁷

Night Lion researchers spoke with Dissent several times regarding TDO, and in each instance, TDO would always circle back and relay their communications.

Dissent is open and transparent regarding her regular communications with the group.



breaches@securejabber.me: But TDO talks to me a lot.

breaches@securejabber.me: I've been in chat for more than 1000 hours by now, I'd guess.

⁶ https://motherboard.vice.com/en_us/article/qkjpzpx/how-a-hacker-is-gaming-the-media-to-extort-his-victims

⁷ <https://www.databreaches.net/thedarkoverlord-leaks-upcoming-episode-of-orange-is-the-new-black-after-netflix-doesnt-pay>

2.6

GROUP FORMATION

FOX OF ST. JAMES, LONDON

In the following thread BlackBox, user 'johnnycornbread' (JCB) discusses accessing the 'Fox of St. James', a Cigar shop in London (www.jjfox.co.uk). Cyper assists in hacking the site. Once the site is hacked, JCB and Revolt develop a ransom note to extort the shop.

This extortion may mark group's first 'team' extortion. Ransoming websites was not a new concept, but this thread appears to be the first time the members joined together and on a target.

This thread includes comments from the following six actors: Johnnycornbread, Cyper, Revolt, Hexxxx, Gingervitis, Zer0ing (four of which are believed to have played an active role in the group).

Author

johnnycornbread

Moderator

Black Hat Hacker

moderator

Posts: 540

Skillz: 31

[Good] [Bad]

Topic: fox of st james (Read 79 times)

Re: fox of st james

< Reply #15 on: >

Cyper - I know you seen this. Are you not helping for a reason? If you not want to help maybe you can tell us what to do?

Cyper

Administrator

Black Hat Hacker

founder

Posts: 914

Skillz: 38

[Good] [Bad]

i am a freaky girl

Re: fox of st james

< Reply #17 on: >

QUOTE

2mins 😊

upload with teh image uploader

<http://www.jjfox.co.uk/images/prodimages/cont.php>

pw: fuck

<http://www.jjfox.co.uk/admin/cont.php>

pw: fuck

funcs.php

function getdbresults(\$sql) {
 \$dblink=mysql_connect("localhost", "jjfox", "dsf78ew");
 mysql_select_db("jjfox", \$dblink);

search for more logins ...

upload more backdoors - get a shell ...

😊

<http://www.jjfox.co.uk/admin/test.php>

Server information:

Server: www.jjfox.co.uk

Operation system: Windows NT CP5-9110 6.1 build 7600 (Microsoft Windows [Version 6.1.7600])

Web server application: Microsoft-IIS/7.5

CPU: Intel64 Family 6 Model 62 Stepping 4, GenuineIntel

Disk status: Used space: 0 B Free space: 0 B Total space: 0 B

User domain: WORKGROUP

User name: IUSR_jjfox

Windows directory: C:\Windows

Sam file: Not readable

PHP version: 5.2.17 (more...)

Zend version: 2.2.0

Include path: ., C:\php5\pear

PHP Modules: bcmath calendar com_dotnet (0.1) ctype date (5.2.17) filter (0.11.0) ftp hash (1.0) iconv json (1.2.1) odbcc (1.0) pcre Reflection (0.1) session ilbxml standard (5.2.17) tokenizer (0.1) zlib (1.1) SimpleXML (0.1) dom (20031129) SPL (0.2) wddx xml xmlreader (0.1) xmlwriter (0.1) cgi-fcgi curl gd gettext imap mbstring mcrypt mime_magic (0.1) mssql mysql (1.0) mysqli (0.1) openssl PDO (1.0.4dev) pdo_mysql (1.0.2) pdo_sqlite (1.0.1) soap sockets SQLite (2.0-dev) xsl (0.1) zip (1.8.11)

Disabled functions: Nothing

Safe mode: OFF

Open base dir: OFF

DBMS: MySQL MSSQL SQLite MySQL

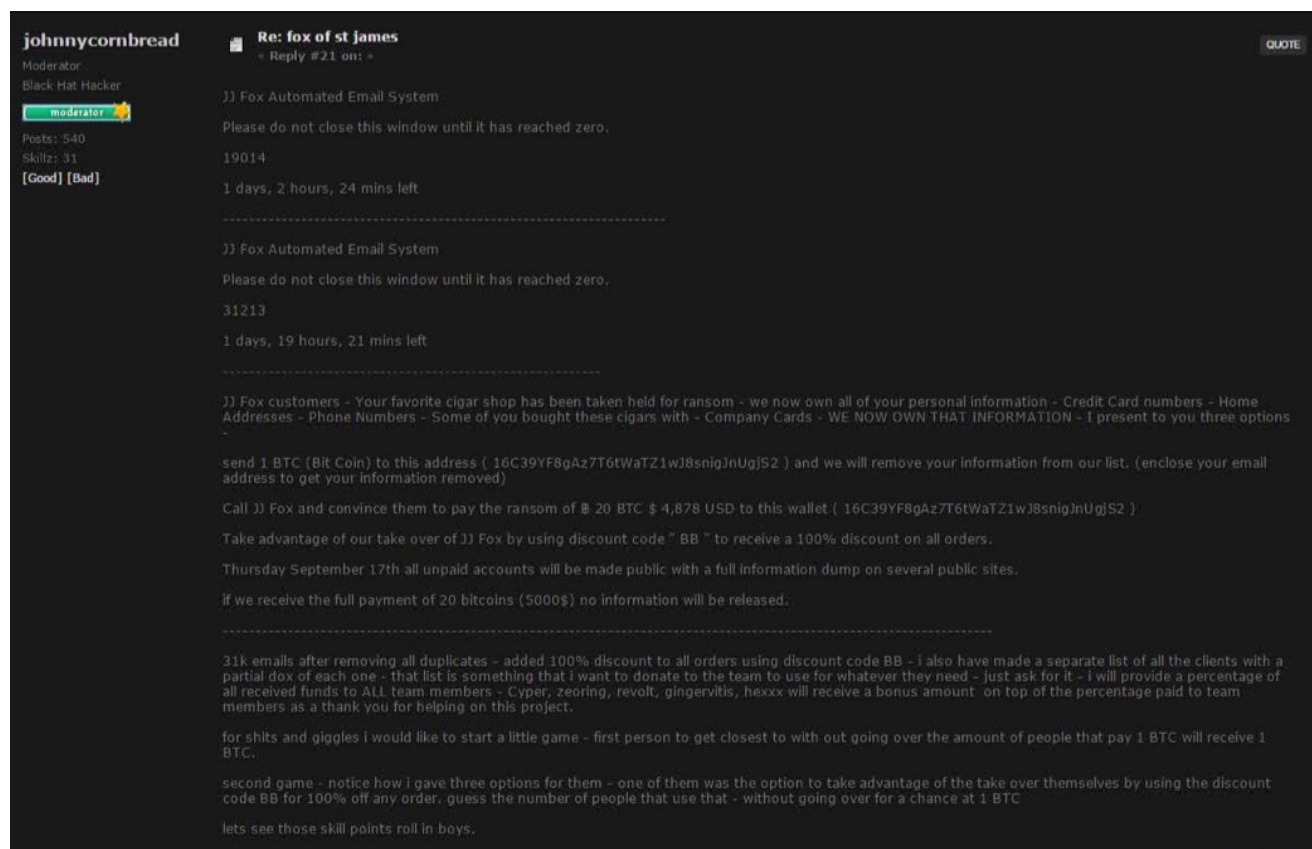
PRE-TDO: A GROUP RANSOM PROJECT

Following Johnnycornbread's request for assistance from 'someone that can write proper english', the JJ Fox of London's website was taken down and replaced with a ransom note.

While there is nothing new or novel with this approach to website ransom attacks, this was the first record of this group of individuals coming together for a group project.

Johnnycornbread also wrote the following

*i will provide a percentage of all received funds to ALL team members - **Cyper, zeoring, revolt, gingervitis, hexxx** will receive a bonus amount on top of the percentage paid to team members as a thank you for helping on this project.*



Note: Cyper, Revolt, and Gingervitis will all be discussed in subsequent sections of this report, and are all members of the TDO collective.

2.7

TDO'S FIRST APPEARANCES

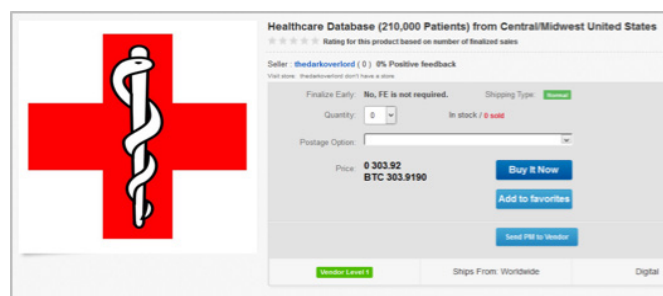
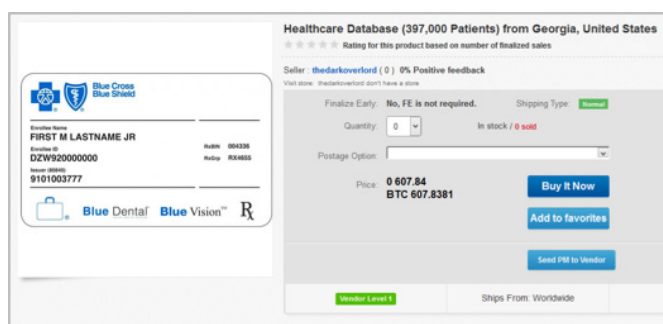
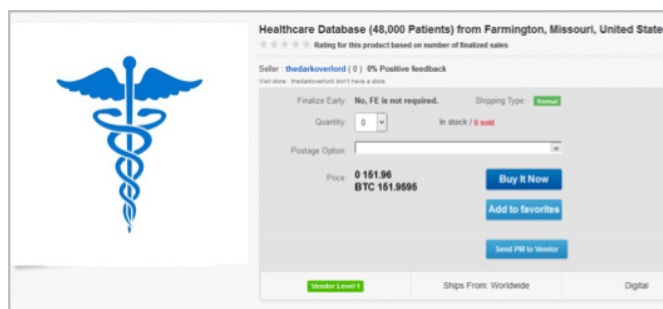
2016 MEDICAL BREACHES

Circa June 2016, “The Dark Overlord” lists 3 separate databases containing a total of 655,000 healthcare records on TheRealDeal (TRD) marketplace. The three databases included: Midwest Orthopedic Clinic, Prosthetic & Orthotic Care (PandoCare), and Athens Orthopedic Clinic.

Within a few weeks of the original posts, a fourth dataset was listed for sale containing insurance provider logins.

FARMINGTON, MO

Worth noting: one of the first major victims of TDO was a group of healthcare clinics in Farmington, Missouri, which is also the residence of actor JohnnyCornbread.



2.8

The members of TDO initially published the sale of medical records on a number of hacker forums, including Hell Reloaded and Exploit. These posts reveal **Arnie, Cr00k, and F3ttywap** as the initial set of TDO threat actors. **NSA(@rows.io)** was revealed shortly after by way of the Louisiana DMV hack.

ARNIE

The 'Arnie' moniker made his first appearance on Hell Reloaded. Arnie was only active for a few months using this name but quickly became known as the group's leader throughout the security community and underground forums.


The following is a snippet of Arnie's introduction post on Hell Forum on April, 2016:

Admittedly, I am mostly a script kiddie. But, we must all start somewhere right? I am here to learn new ways to profit through information gathering and attacking my targets through whatever non-violent means possible. I have successfully used SDR to steal shit out of garages, steal cars, and even broke the ACS of a bank building. I have even used a combination of radio jamming gear and a spectrometer to jam and identify anti-theft devices with the intention of safely being able to boost a car. I am a big fan of hardware hacking and have successfully been able to penetrate businesses by doing what I call USB bombing.

Within a few months, Arnie made the following posts titled 'RDP access to medical providers', advertising the sale of TDO's first major data heist.

Author

arnie
VIP
First Feedback



NAME: RND
(unread post)

Topic: RDP Access to an Entire Medical Group (Read 7 times)

RDP Access to an Entire Medical Group

I am interested in selling my access that I have. I recently came across some PDF credentials for a clinic group in the central US that has several offices. With this PCP access I have done some stealthy snooping and have determined that this is a nice little gold mine. I am not interested in hitting this one myself as I have too many other projects going on but I am interested in seeing if you body guys are interested. As far as background goes, this is a medical clinic group in the central US who works mainly in sports medicine and orthopedic related practices. They have a fairly well established client base with a constant upturn of new clients coming in. There is a lot of data to be generated from this access. I am going to keep the details to a minimum at the moment, but any serious buyer is welcome to PM me and I will provide further details, but only if you offers letters to vouch for you. I do not want any reporters or possible LE getting wind of this one.

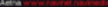


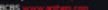
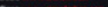

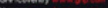
Here is a single screenshot to show that it has access to the facility and a brief list of some of the types information I have come across.
[http://tiny.cc/meywDkpw](#), [http://tiny.cc/qvz9Dkpw](#)

A little about the machine and LAN:
The machine is a standard core i7 processor, but you can easily exceed yourself to a local administrator immediately available on the machine, are four accessible hard drives containing ~3TB of total data. The machine is running Windows Server 2008 SP2 Standard SP1. It is being run on a Intel X3430 CPU @ 2.4Ghz with 3GBS of ram and of course this is your good ol' 64 bit version of Windows. As for software goes there is an ERP in main database files stored in plaintext. In the ERP are things like Patient list, Providers, Email, Chiroprag, Demographics, Phone Numbers, SSN, DOB, Address, Medical records, Reports, MRI's, X-Rays, Billing information, Transaction history, etc. On this machine there are roughly forty-five total users whom are all the local staff. Many of which are orthopedic doctors.

A straight forward ar-scan came up with a client list about fifty strong, if I had to eyeball it and take a good guess. This was done during off hours so as to not raise any attention because there is a monitor attached with this machine. During the day you may find many more machines and devices connected. I have taken the time to do a report and brief analysis of the local machine and the immediate surrounding network so I took care to not reset... nah, refresh show state, refresh firewall show config, tasklist /svc, and net stat as basic means to collect quickly obtained data. I have screenshots of all of this information and will make it available for any prospective buyers.

As mentioned before, if you want more information you WILL need to be vouched for to receive it or have a lot of money to talk me into it. I am more than happy to do anything the address and will even allow the address to PCP in to confirm the state of the machine and the client I have made, so long as this is done stealthily and in the off hours of the business. I have intentionally not listed a price for this as I am very negotiable on this. This will definitely not be any less than 10 BTC though, so do not PM asking me if you can buy for 1 or 2 BTC.

"Quality is never important here speedily. Our focus is to reach those who are leaders". - Steve Jobs

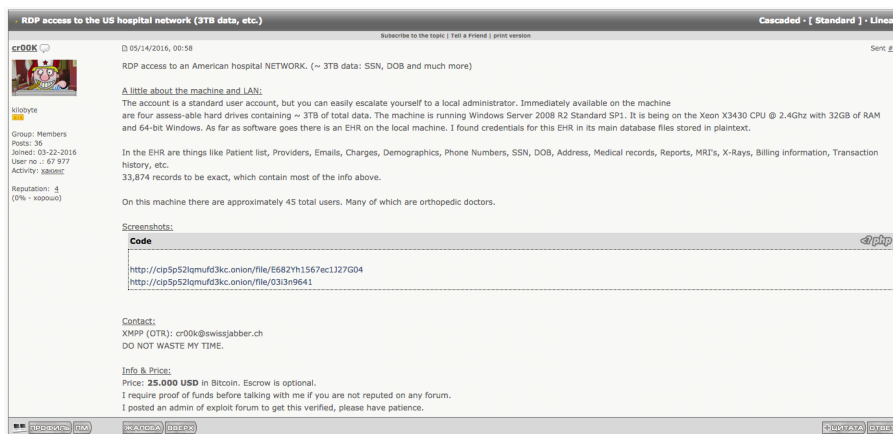
	
These logos to the provider portals for the following insurance companies	
	Aetna www.aetna.com AM www.provider.aetna.com Availity www.availity.com
	BCBS www.bcbs.com Cigna www.cignaplanet.com GPCoverity www.gpc.com
	Humana www.humana.com MCAD (website hidden for now) NIA www.niafco.com
	Noridian www.noridianconnect.com One Call www.onecallmed.com Optum www.cloud.optum.com
	Paycom www.paycomhealth.com PNC www.pnc.com/medicare/medicaid TriCare www.tricareonline.com
	UHC www.unitedhealthcare.com UMR www.provider-itsa.com

CROOK

On the Russian hacking forum Exploit, user cr00k posts similar TDO data providing cr00k@swissjabber.ch as his contact information.

User cr00k posts similar 'medical data' for sale on KickAss, using the same contact information.

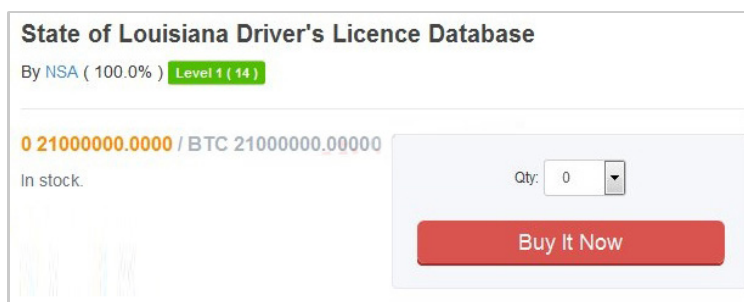
Identical posts were made on Siph0n forum under user F3ttywap, contact address w4p@exploit.im.



NSA

NSA (nsa@rows.io) became known for advertising the sale of hacked records from the Louisiana Department of Motor Vehicles on TheRealDeal market.

Note: rows.io is NSA's XMPP contact address and not part of his name.



In the following private Twitter conversation, TDO (@tdohack3r) admits being the person responsible for the Louisiana DMV hack (recipient text removed).



THE DARK OVERLORD
@tdohack3r

TDO: you know LA DL hack?
TDO: i did that 336,847,320 from US gov
TDO: i am biggest hacker in world
TDO: look up LA DL 290k hack
TDO: i hack 290k LA DL records
TDO: all over news
TDO: they not pay me yet but they want to right now
TDO: i can prove it
TDO: if you dont believe me
TDO: i am the most elite hacker in the world right now
TDO: i hack world biggest DB from US gov
TDO: and you say i find RDP cred on public server
TDO: ahhahahahahahahah

2.9

DE-EVOLUTION OF THE GROUP

TDO's methods for infiltration and extortion changed after 2017. TDO's original leadership focused on extorting victims gained by hacking, and appeared to be significantly more organized. Following the leadership change announced in 2017, the group's methods began to devolve, moving away from hacking and focusing on fake extortion attempts and outright terror.

EMPTY EXTORTION

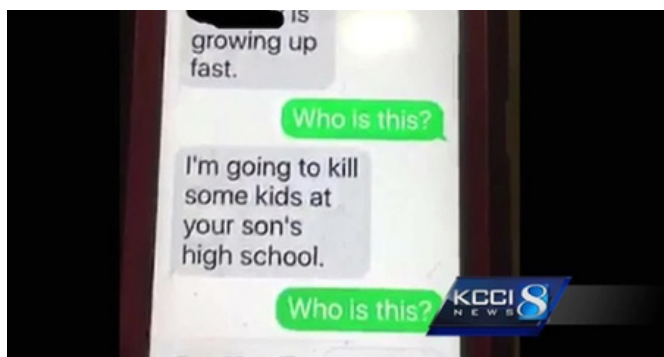
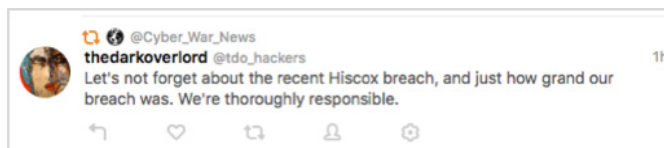
A number of organizations reported being contacted by TDO even though they were never breached. During one of their first breaches, TDO obtained copies of Business Associates Agreements (BAA) between a victim and several of its medical providers.

TDO would then contact those medical providers claiming they had been breached, offering non-existent or recycled patient information as evidence of their access.

TERROR AND VIOLENCE

In 2017, "TheDarkOverlord Solutions" switched their tactics to outright terror and began threatening the welfare of students. Text messages were sent to parents threatening the life of their children.⁸

The initial threats to the Colombia Falls School District resulted in the disruption of more than 30 schools over a 5-day period. TDO even went as far as to write the SD6 board of trustees a 7-page ransom note.⁹



⁸ <https://www.grahamcluley.com/hackers-school-student-data/>

⁹ <http://1qb1ow3qfudf14kwjzaxq61.wpengine.netdna-cdn.com/wp-content/uploads/2017/09/Letter-with-redaction.pdf>

2.10

COMMUNICATING WITH TDO

September 2018, following an article that publicly outed a Night Lion researcher as 'SoundCard' ¹⁰, TheDarkOverlord (@tdo_hackers) agreed to communicate over XMPP (Jabber chat).

TDO was approached under the premise that this researcher was upset over the article, and was interested in working with TDO to make extra money. During the initial conversation (over Twitter), the researcher mentioned approaching NSA (aka Cyper, admin of KickAss) to post stolen material.

TDO began the conversation by immediately asking about NSA.

VT: So how are things in overlord land?

4vmc3txofm: You mentioned NSA's name.

VT: i don't believe i did?

4vmc3txofm: "You have the marketing pull and the ability to get media's attention. that's what i'm after. My backup would be to go to NSA but i dont think he can create the same buzz you can."

VT: Oh

VT: right

VT: KickAss.. I posted my data to KA, but not great response. looking for better outlets

4vmc3txofm: Is that so?

VT: So what about NSA?

4vmc3txofm: What about him? You mentioned their name.

VT: I didnt realize NSA was a They. I was just suggested i go to him and see if he can help move the data. I was more interested in working with you though

4vmc3txofm: Why is that?

VT: Because you are the great and powerful Oz. You know why, stop fucking with me.

¹⁰ <https://krebsonsecurity.com/2018/10/when-security-researchers-pose-as-cybercrooks-who-can-tell-the-difference/>


2.11

TDO APPEARS ON KICKASS

Following the conversation with Night Lion's researchers, TheDarkOverlord appears on KickAss, and over the course of the next 3 months, will continue to use that forum to promote their merchandise.

thedarkoverlord Is Here

Thread Modes



thedarkoverlord

Junior Member

Progress: 33%

Posts: 14
Threads: 4
Reputation: 0
Level: 2 [★ ★]
Total Points: 4
Rank 3 / 37
93% to upload Level
Activity 4 / 4
3% to upload your Rank
Experience 50
50% to upload Experience

09-19-2018, 12:29 PM

#1

Indifferent fraudsters, horrified onlookers, and aficionados of obtaining involuntarily divulged information,

We're going to have your interests piqued in just the right spots with our appearance here on KA. In our usual fashion, we come bearing forbidden fruits in the form of deliciously tasteful data and information that even the worst of you will find appetising. Dozens of terabytes, for anyone counting, and we're willing to share with the world.

For those of you who live in the Nothern Hemisphere of planet Earth, Summer has come to an end and Autumn has arrived. Soon, the deciduous trees will be stripped nude with their discoloured leaves falling to the ground. Many creatures will begin to prepare for their hibernation in Winter, eating and then gaining body fat (similar to humans during the holidays which are celebrated during this time of year). However, the creatures that make up thedarkoverlord do not hibernate, sleep, slow down, pause, or stop. For they work around the clock, pillaging and taking whatever they desire or seeping through the cracks of the foundation of the unlucky entity they targeted, weaving into them undetected and striking with surgical precision. We noticed that thedarkoverlord has apparently breached many more entities. After conducting an internal audit to determine just how surgical thedarkoverlord has been this year, we learned that we're certified neurosurgeons.

What does this mean for all of you? It means that we've been so busy and successful that we're now sitting on terabytes of stolen loot. This stolen loot needs a new home amongst the likes of our fellow fraudsters, hackers, and thieves; you all. This serves as our official announcement that we'll begin commencement of our dark web sales campaign that is designed to arm the likes of you all with some of the most desirable and dangerous loot of the current era. With great power comes great responsibility, and that's why there's no better place for our hard earned data and information, than in your hands.

On another note, we've been bearing witness to several incidents where our good reputation and name has been used by individuals whom are operating under our name without authorisation. Although we applaud the individuals for their successful breaches (despite how boring SQL injection and the acquisition of non-PII data is) and the clever act of pinning this all against us, we do not appreciate the unauthorised use of our name. Unlike some laughable and inadequate actors, we are not an "idea" or a "collective" and as such, one shouldn't operate under our name in order to uphold one simple and easy to follow concept: Honour Among Thieves. Be advised that no true members or associates of the thedarkoverlord operate without our express written consent and declaration.

Your new friends,
thedarkoverlord
Professional Adversary
World Wide Web, LLC

Over the course of the next 3 months, TDO continues to advertise the KickAss forum in order to drive up interest to charge a \$600 membership fee.

 **TWITTER** 17m ago

thedarkoverlord Tweeted:
If you're on KickAss, we're about to post some death vids as the result of a USA defence contractor doing a Navy project.

THE END OF THE DARK OVERLORD

THE 9/11 PAPERS AND KICKASS EXIT SCAM

Following TDO's public appearance on KickAss, all future correspondence would be tagged with a link to the KickAss forum.

thedarkoverlord E-Mail Address: tdohackers@protonmail.com

Backup1 E-Mail Address: thedarkoverlord@msgsafe.io

Backup2 E-Mail Address: thedarkoverlord@torbox3uio6wchz.onion

KickAss Tor Address: kickassugvgoftuk.onion

The address of the KickAss forum being promoted by TDO "kickassugvgoftuk.onion" was an old address of the forum that had not been in use for close to a year.

On December 31, 2018, The Dark Overlord began a series of tweets and posts that he would be releasing privileged legal documents regarding the 9/11 terror attacks. TDO claimed "5 layers" of documents, and each layer would be unlocked once new ransom demands were met. The second layer of documents were released exclusively on the KickAss forum, which by now was charging \$600 per registration.

On Jan 08, 2019, a seizure notice was placed on the old KickAss URL. All current URLs were taken offline (or changed for a 4th time in the past year). All paid members were essentially kicked off the site and not given the new URL.

ANALYSIS

The blatant and consistent advertising of KickAss by TDO was nothing more than an exit scam. TDO lured new members to KickAss, requiring a \$600 membership fee in order to gain advanced breach documents (such as the 9/11 papers). After a short time, the site was replaced with a phony seizure notice, the URL changed once more, and all paying members removed.

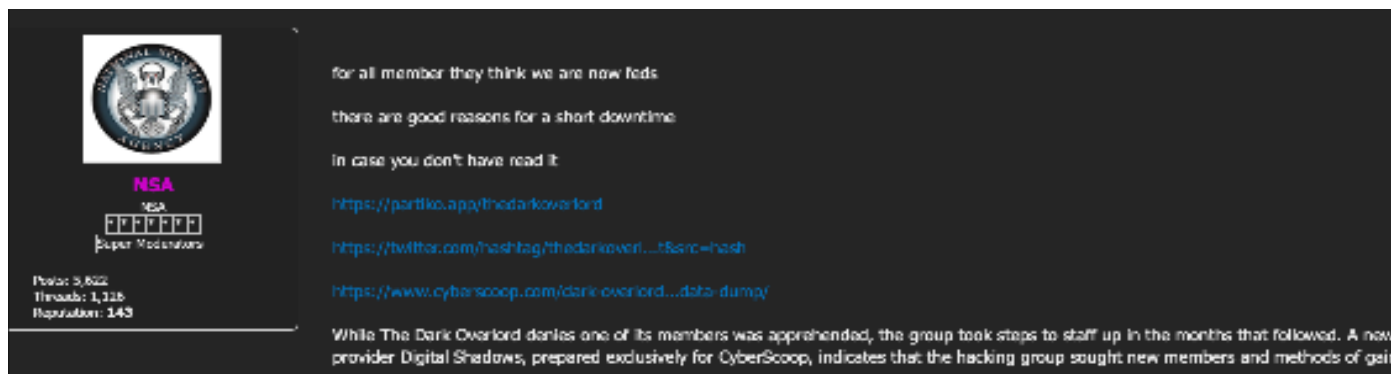
This is the exact tactic and seizure notice used when Cyper shut down his BlackBox forum in 2017.



POST-MORTEM

THE KICKASS FORUM SURVIVES... FOR A WHILE

Following the fake seizure notice, the forum re-starts on a new/private URL and admin NSA posts a message regarding the site's apparent closure.



A CONVERSATION WITH A DIFFERENT THREAT ACTOR

Circa July 2019, an associate had the following conversation with a different threat actor and sent me a copy of the logs.

```
X:      u know if kickass is back yet?
X:      i cant find NSA or inferno anywhere
XXX:    Imo, kickass isn't coming back
X:      oh
X:      they start a new site?
X:      or all the TDO shit?
X:      it looked like they were exit scamming
XXX:    With all the shit that went down with krebs/troy everythings on pause
XXX:    I think it was tdo related
X:      what went down with krebs / troy?
XXX:    Thats what I heard anyway
XXX:    well
XXX:    less them, more that guy Vinny troya
XXX:    troia*
X:      oh the article
X:      gotcha
```

We certainly did not mean for KickAss to be shut down. Sorry!



Section 3

The Dark Overlord

Breach Statistics

3.1

RESULTS SUMMARY

OVERVIEW

The breach statistics provided in this section will show a more complete picture of the cyber crimes committed by the threat actors and groups discussed in this report.

The results only consider data breaches which occurred between January 01, 2017 and June 30, 2020, and **do not include losses involving the theft of credit card data** (e.g., Home Depot). All breach figures, sources, and calculations used in the development of these statistics are provided for complete transparency in this report's index.

METHODOLOGY

In addition to the crimes committed as "The Dark Overlord", this report will also show the two primary threat actors engaged in additional crimes under different group names including ROR[RG], NSFW, Gnostic Players, and Shiny Hunters.

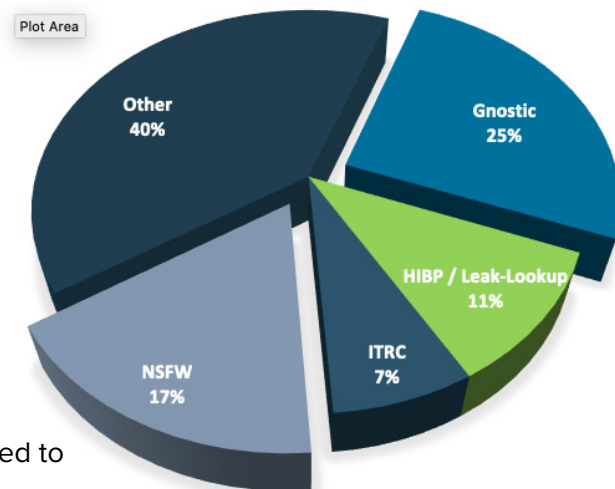
The data analysis is thereby broken into specific categories to show the percentage of overall breaches committed in that year by each specific group. The following additional sources were references to ensure completeness and accuracy of the results:

- Identity Theft Resource Center (ITRC)
- Have I Been Pwned (www.haveibeenpwned.com)
- Private vendor sale lists
- Leak-Lookup.com
- Media outlets (breach stories)

RESULTS

Between the periods of Jan 2017 and June 2020:

- Groups NSFW and Shiny Hunters can be directly attributed to 17% of all data breaches during this time period
- Gnostic Players accounts for 25% of all data breaches during the same period
- Because of their involvement in both groups, the same **two actors described in this report** can be directly tied to **42% of all data breaches** over this time period.



3.2

DATA ANALYSIS

All figures provided in the results sets provided as millions of records breached by source.

RESULTS SET 1

The breach figures provided in Set 1 also include breaches (or data leaks) disclosed by security researchers with no malicious intent.

Source	2017	2018	2019	2020	Total	%
Gnostic	311	771	737	0	1,901	16%
HIBP / Leak-Lookup	140	304	80	60	804	7%
ITRC	16	32	64	80	535	4%
NSFW / ShinyHunters	0	222	504	536	1,283	11%
Other	301	1,721	110	949	2,971	25%
Researchers	393	637	1,496	0	4,373	37%
Total	768m	3,786m	2,991m	1,625m	11,867m	100%

RESULTS SET 2

The breach figures provided in Set 2 only include data breaches by malicious actors.

Source	2017	2018	2019	2020	Total	%
Gnostic	311	771	737	0	1,901	25%
HIBP / Leak-Lookup	140	304	80	60	804	11%
ITRC	16	32	64	80	535	7%
NSFW / ShinyHunters	0	222	504	536	1,283	17%
Other	301	1,721	110	949	2,971	40%
Total	768m	3,049m	1,496m	1,625m	7,494m	100%



SECTION 4

The Dark Overlord

Actor Profiles

4.1

THREAT ACTOR MATRIX

The following matrix contains a summary list of TDO members and associates, as well as a small list of their aliases. A complete list of known aliases is included in their respective sections.

	Actor	Role	Aliases (Partial)	Real Name	Location
4.2	Cr00k	Sales, Hacker	f3ttywap Ping Photon Russian	Dennis Karvouniaris	Calgary, Canada
4.3	Peace of Mind	Group Leader	NSFW Revolt NSA Megadimarus Stradinatras WhitePacket	Christopher Meunier	Calgary, Canada
4.4	Arnie	Hacker, Patsy, Public Lead (TDO1)	CraftyCockney Gingervitis JasonVoorhees Mari0 Mas	Nathan Wyatt	United Kingdom



4.2

Name: Dennis Karvouniaris (DK)

CROOK

Age: 18 Location: Calgary, Canada

ALIASES

c86x
dio_the_plug
F3ttywap
Jinn
Lava
Malum
Nakk3r
NSFW
Overfl0w
Photon
Ping
Rejoice
ROR[RG]
Russian
Ryder

AFFILIATIONS

Hell (Founder)
TheRealDeal
NSFW
Gnostic Players

JABBER IDS

c86x@blackjabber.cc
chms@jabber.se
cr00k@swissjabber.ch
ping@rows.io
russian@xmpp.is
sepa@swissjabber.ch

SOCIAL MEDIA

instagram.com/dio_the_plug

SUMMARY

Dionysius "Dennis" Karvouniaris (DK) aka Ping, was the original owner of Hell Forum. DK was also known HA, ROR[RG], Rejoice, and Ryder on Hell Reloaded. DK is well known as a data broker and trader and is known for working with members of the media to help further his sales goals. DK used the persona Cr00k and f3ttywap while selling TDO related data, and has since been involved with a number of additional hacks under the alias NSFW currently hacking under alias NSFW with the group Gnostic Players.

TACTICS

This threat actor likes to create confusion and deception by stealing the handles of known hackers. DK will often use the press to gain attention for his forums and the merchandise he is involved with trafficking.

He is also a master at using the media for manipulating events and throwing law enforcement off his trail. DK will create fake scenarios, publish fake doxes, and manipulate conversations to create stories designed to send investigators down endless rabbit holes of incorrect information.

4.2.1

ROLE IN TDO

MARKETING & SALES

Similar to his history of selling data breaches, Cr00k was most notably a sales mechanism for TDO. It is believed that Cr00k also shared in duties related to answers and managing TDO sales accounts. Cr00k's connection to the TheRealDeal marketplace (as an admin) provided TDO with a centralized location to publicly advertise and sell their goods.

In the following private conversation, user c86x, a known TDO broker, admits to being Cr00k.

```
c86x:      I have 3 DB's, those formats are on my sales thread
c86x:      I was asking which format
c86x:      but here you go
c86x:      "25865","Keith","Goldacker","486-70-9603","1259 Weathergon Place",,
           "Bawin", " MO","63021","636-256-7462","kgoldacker@charter.net","09/30/2015",
           "DELAFO",,, "09/30/2015", "10/07/195 7","CIGNA","U45226427-02",,"KARGAS",
           "DAVID","KARGES","DO","LB","L1970","1818.03"

c86x:      PatID,FirstName,LastName,Soc,Addr1,Addr2,City,State,Zip,HomePhone,WorkPhone,E
           mail,LastAppt,Date,LastVisit Type,NextApptDate,NextVisitType,LastDOS,FollowUp
           Date,BirthDate,Ins,InsID1,InsID2,RefPhysCode,First,Last,Title,LastPract,LastBase,
           LastTotal

xxx:      hey man...saw it before
xxx:      got a few of those
xxx:      cr00k sells same shit
c86x:      I'm cr00k
xxx:      LOL
c86x:      hese are the test samples, for purchasing I direct you to my partner so you can work
           with escrow without any problem

xxx:      prote3 from hells?
c86x:      I don't know if he was on that forum
c86x:      know him from DK
c86x:      just don't tell everyone I'm cr00k, I like to have things seperated
```

4.2.2

ATTRIBUTION

CONNECTING DK WITH
CR00K, AND TDO.

ATTRIBUTION SECTIONS

A. Linking Cr00k with Prometheus

B. Additional Attribution Between Prometheus to TDO

C. Connecting Prometheus to NSFW and Photon

D. Connecting NSFW to Ping and Cr00k


E. Who is the Real Ping?

4.2.2.A

LINKING CROOK TO PEACE OF MIND AND PROMETHEUS

The following chain of events will show a timeline connecting aliases cr00k and Peace of Mind.

1. Article posted on KA regarding a hacker's breach into a number of porn sites, such as Team Skeet.



NSA •
Super Moderator
founder

Posts: 4,483
Threads: 981
Reputation: 106
Level: 50 []
Total Points: 45,061
Rank 122 / 1227
92% to upload Level
Activity 1,529 / 45061
98% to upload your Rank
Experience 9
91% to upload Experience

04-02-2016, 02:42 PM


Hacker Breaches Porn Network, Advertises User Data on Dark Web

A hacker has gained access to administrative functions on the porn website Team Skeet and is advertising a database supposedly containing email addresses, plain text passwords, names, and physical and IP addresses for over 237,000 users of the site, as well as the broader porn network, Paper Street Media (PSM).
The hacker, who is selling the alleged data under the handle TheNeoBoss on the Dream Market, told Motherboard in an encrypted chat.


Last week, Motherboard was provided with an initial sample of 64 users. Out of these, 56 were seemingly linked to real Team Skeet accounts, as the website read, "Sorry that username is unavailable." The hacker then shared a larger set of data with Motherboard, containing over 8,000 credentials, and Motherboard checked that many of these apparently corresponded to accounts on the site. TheNeoBoss also sent a screenshot indicating that he was in possession of some 237,000 users, but Motherboard has been unable to confirm whether that is the case.

Usernames that were apparently linked to real accounts on Team Skeet also worked on several other websites in the PSM network, which Team Skeet is a part of. These include Eextra Small, Teen Pies, Innocent High, Teen Curves, and CFNM Teens. The Team Skeet website says that members can get access to 23 separate sites.

Some of the email addresses failed to receive messages, however, when Motherboard attempted to contact their owners. And some of the entries in the sample data did not include physical addresses. The hacker claimed to have access to some credit card data, but did not take it.



2. User cr00k selling Team Skeet (and other) data on KA.



cr00k •
Banned
failed

Posts: 93
Threads: 14
Level: 9 []
Total Points: 170
Rank 20 / 205
92% to upload Level
Activity 34 / 170
81% to upload your Rank
Experience 20

03-29-2016, 12:36 AM

List of DB's for sale.

CardingMafia.ws feb 2016 full DB includes everything, 177k users vB hashes & private messages.

ArmyForceOnline.com game network Feb 2015, 2m users, MD5 hashes.

TeamSkeet.com USA porn network, some name/address/city, around 400k users & plaintext passes.

forums.kmplayer.com, vB hashes 434k users, dumped Feb 2016

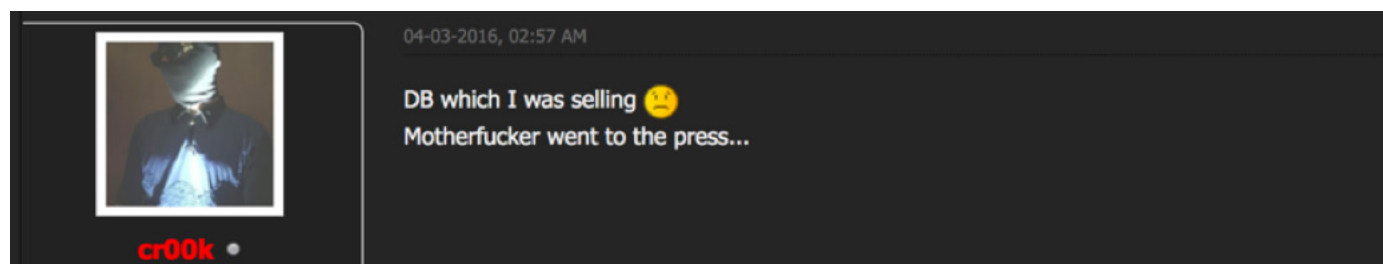
DotaHut.com forum, 118k users, dumped Jan 2016

BotOfLegends.com November 2014, 236k users

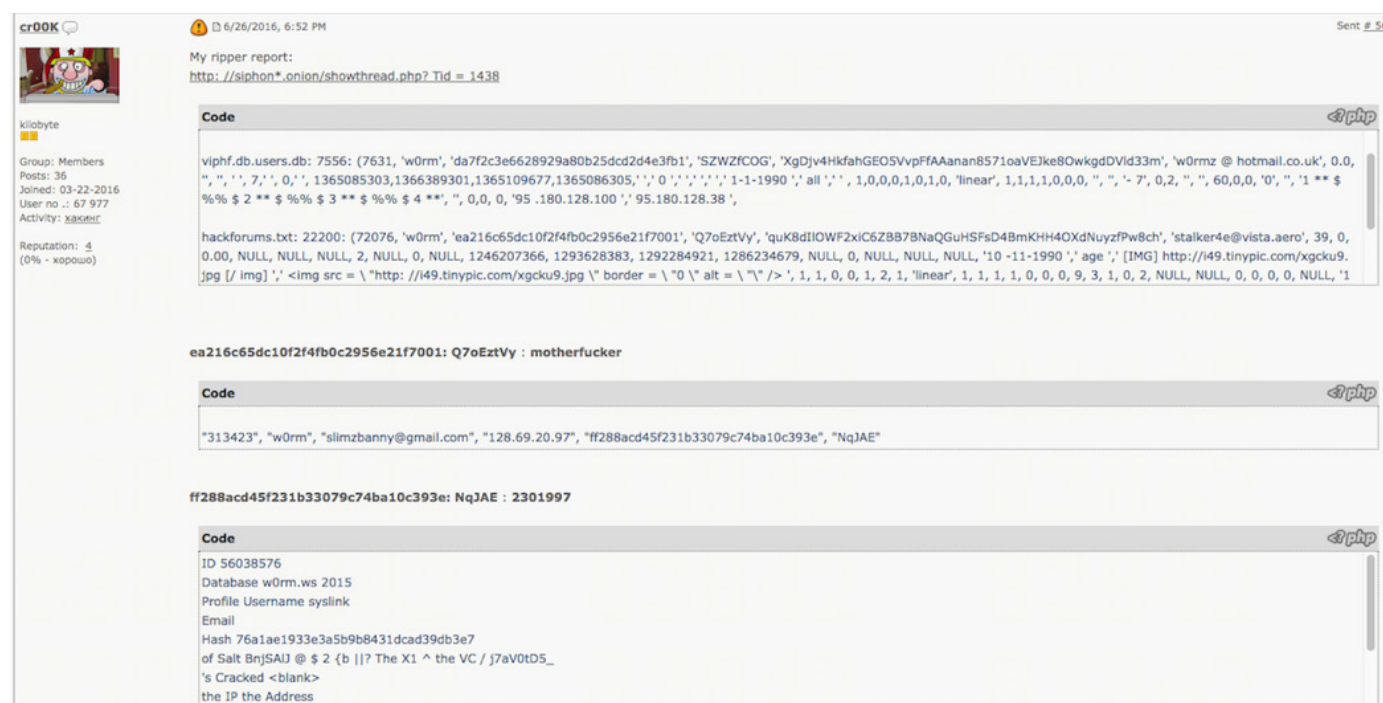
Jabber ID: cr00k@swissjabber.ch

No set prices, please offer me in Bitcoin.

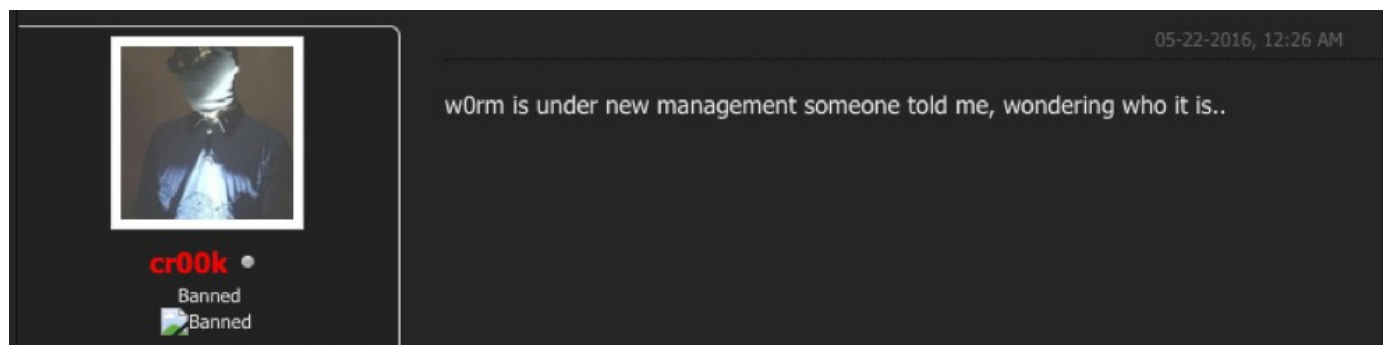
3. User “NeoBoss” (aka Worm) contacts Joe Cox of Motherboard and takes credit for the hack.¹⁴ Worm publicly released the database that cr00k was selling, effectively making it worthless.



4. User cr00k files ripper report against Revolver (aka w0rm) on Exploit forum. An exact ripper report was posted on siph0n by user f3ttywap (also DK).



5. May, 2016, Cr00k posts a message on KickAss forum that w0rm.ws site is under new management.



¹⁴ <https://nakedsecurity.sophos.com/2016/04/05/free-porn-for-life-using-stolen-teamskeet-accounts-advertised-on-dark-web/>

6. October 2016, w0rm's forum is hacked and defaced as retaliation for publishing cr00k's data. The site defacement reads: "Hacked by Peace of Mind and Prometheus for fucking with Hell Forum".



7. Oct 04, 2016: Peace of Mind takes credit for w0rm hack in Motherboard Article.¹⁰

"He decided to fuck with me so I [ended] up getting root on his box," Peace told Motherboard in an Online chat.

"Peace wouldn't go into the specifics of why he had targeted w0rm. When asked if it was because w0rm had scammed him over a database sale, Peace said, "sort of, yes."

"[w0rm] was reporting [vulnerabilities] of websites I had access to. I ended losing access cause of him."



¹⁰ https://motherboard.vice.com/en_us/article/mg75ea/hacker-linked-to-myspace-linkedin-dumps-hacks-competitor

8. Analysis of leaked w0rm.ws database shows takeover announcement, "W0rm is under new management, send payments and info to ke7hb@w0rm.ws".

```
--  
-- Dumping data for table `announcement`  
--  
  
INSERT INTO `announcement` (`announcementid`, `title`, `userid`, `startdate`, `enddate`, `pagetext`, `forumid`,  
`views`, `announcementoptions`) VALUES  
(1, 'Trusted Section', 'w0rm is under new management, as you can see there will be launched a section named  
"Trusted" which only will be available to the most elite members and/or contributors.  
Payment & info: ke7hb@w0rm.ws', -1, 365, 29);
```

9. Logs from leaked w0rm.ws forum show the following message sent from ke7hb on May 28, 2016 (several months before the forum hack), asking to be contacted at data2z@swissjabber.org (a known TDO address).

```
(3049, 2508, 3048, 'ke7hb', 386, '', 1464451741, 'hi, I have contact for traffic \n  
[email] data2z@swissjabber.org [/email] is my temp jid.', 1, 0, '85.25.103.69', 0, 0, 0, 0, 0),
```

10. Viewing the database's change log shows ownership of ke7hb transferred to user cr00k (crook@swissjabber.ch).

```
--  
-- Dumping data for table `userchangelog`  
--  
  
INSERT INTO `userchangelog` (`changeid`, `userid`, `fieldname`, `newvalue`,  
`oldvalue`, `adminid`, `change_time`) VALUES  
(61, 387, 'username', 'ke7hb', 'cr00k', 100, 1463697364),  
(62, 387, 'email', 'ke7hb@iranmail.com', 'cr00k@swissjabber.ch', 100, 1463697364),
```

ANALYSIS

As retaliation for giving away his stolen data, Cr00k and ke7hb hacked w0rm's private forum. User ke7hb appeared to have moderator privileges, was active on the account for months prior to the hack, and used a known TDO address for communications (data2z@swissjabber.org).

Following the announcement of the forum's hack, ownership was transferred to Cr00k (at user cr00k@swissjabber.ch, a seller of TDO data). The internal drama between the actors resulted in the users publishing a SQL dump of the w0rm.ws forum, allowing us to connect Cr00k with users Peace of Mind and Prometheus.

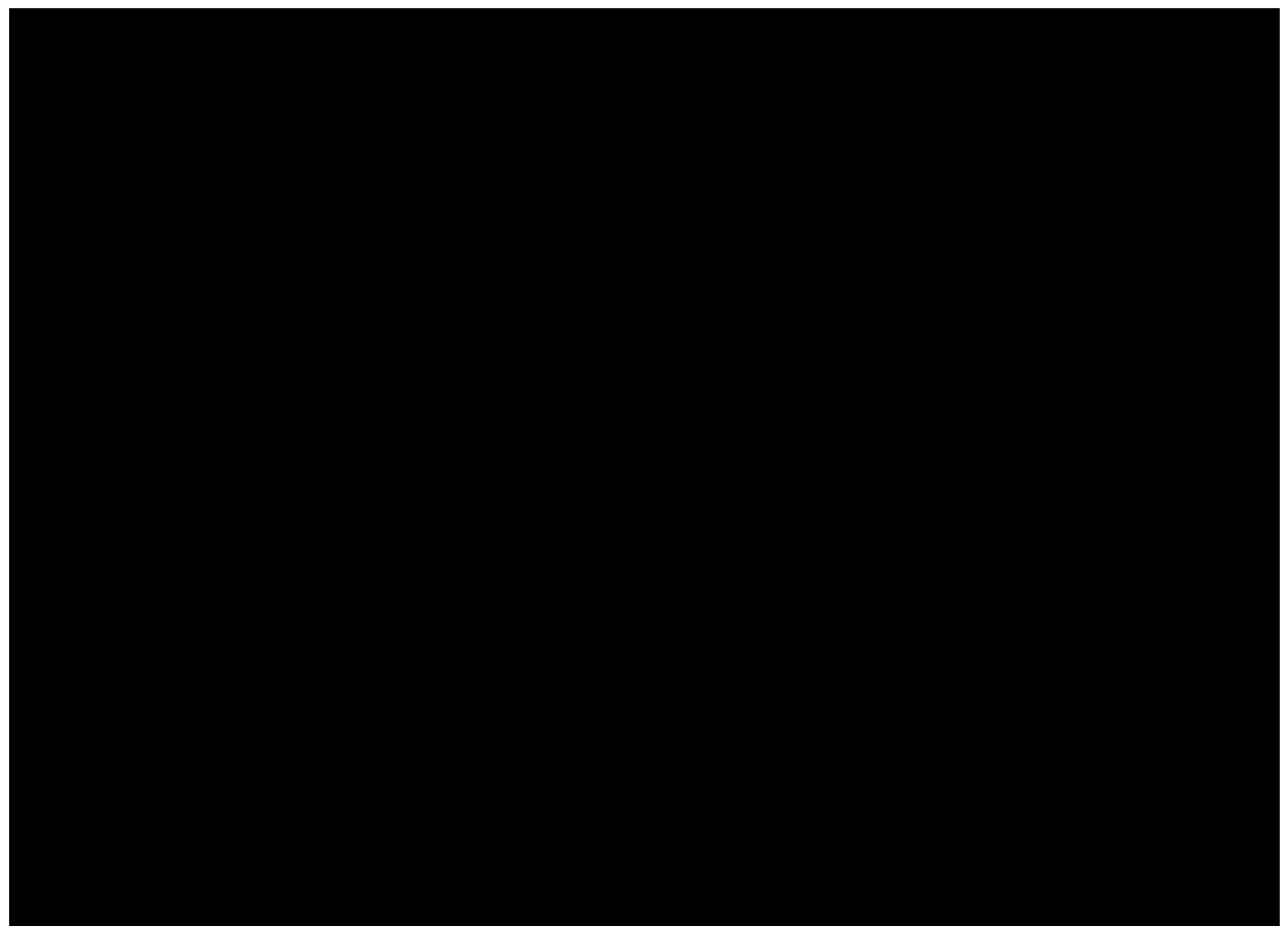
Based on this evidence, ke7hb and Cr00k are associated with Peace of Mind and Prometheus. Subsequent sections of this report will determine which users are connected.

4.2.2.B

ADDITIONAL ATTRIBUTION BETWEEN PROMETHEUS AND TDO

In 2017, a dox of user [REDACTED] sent from a confirmed TDO email address.

When directly asked about this email, and why/how TDO would have a copy of the photos, [REDACTED] angrily admits to having sent the photos to Prometheus.



prometheus is a kid
because he was the only one whom i send this picture to

4.2.2.C

CONNECTING PROMETHEUS TO PHOTON AND NSFW

PHOTON'S INTRODUCTION TO ODAY FORUM


User Photon (Oday forum) has ties to the original Hell forum, most notably a connection to the OPM (Office of Personnel and Management) data breach.

Different threat actors allude to a part of the OPM data breach being available for a short time on the original Hell forum. As the original forum closed, drama befell the group and the data was stolen by Revolt and Cyper from Ping's private repository.

The following is a screenshot of Photon's initial application to the Oday forum, using the email address `assemble@protonmail.ch`.

Accepted Ashwiniscool

Threaded Mode | Linear Mode

Author	Message
<div><div>Photon</div><div>Donor</div><div></div><div>Posts: 150 Joined: Oct 2015 Reputation: 20</div></div>	<div><div>Who invited you or how did you find us?</div><div>Post: #1</div><p>I found my own way to this forum, being fairly new to Tor, I went on the hunt of finding some "real" forums as I am a big name in some of the clearnet forums but all the admins there and users there seem to be complete pricks in general, so I literally moved over to get a new forum life! 🤔 I wanted to see what forums I could get into, I just searched around for a bit, saw forums that claimed to be cool, like this and others and this seemed to look the best so I joined, (or am trying to join).</p><p><u>Links to your profile on similar Tor/Cleartnet forums</u></p><p>As I want to keep my identity safe, this will be a first for me, I have never linked myself to profiles in other forums. So this is definitely a first for me to trust people at.</p><p>My email: <code>assemble@protonmail.ch</code></p><p>I have just got into siph0n with the alias: Photon</p><p>I am the admin of: <code>thepiratecove.org</code></p><p>I am in social engineered with the alias: Ashwiniscool</p><p>bhf.su: Ashwiniscool</p><p>https://forbiddense.com: forbiddense</p><p>nulled.io: Cracked</p></div>

Note: In the same way Cr00k also leads to a carder in Canada, we believe the name Ashwin, aka Ashwiniscool, is a trap to lead researchers directly down the wrong path. Cr00k is highly skilled at associating himself with names that can easily be traced to other people.

A SHARED LINK BETWEEN PHOTON AND NSFW

Evidence suggests DK is one of the two people associated with the name NSFW. Most actors believe NSFW is one person, which is the result of the two members sharing jabber accounts and communication logs, thus making them appear indistinguishable.

When referencing DK as part of NSFW, this report will refer to him as Photon or Russian.

1. In the following private conversation, user Photon is revealed as also being NSFW, Ryder and Prometheus.

XX: NSFW == prometheus == ryder == photon
XX: I don't understand why are you so confused it's so simple
XX: prometheus == script kiddy
ME: NSFW is prometheus?
XX: yes NSFW and prometheus are the same person

2. Contact with NSFW initially began on RaidForums.com. The following screenshot shows a post by NSFW offering his jabber account, nsfw@jabber.se.

NSFW

Thanks.
Contact here or at NSFW@jabber.se

3. Photon's primary Twitter account, @PhotonicProton was used to offer NSFW@jabber.se and Russian@xmpp.is as his jabber addresses.

 **Photon** @PhotonicProton

jabber.se down i added u on russian@xmpp.is

4. When asked about the photos discussed in Section 4.2.2.B, Russian (NSFW) confirms the pictures were sent to him. Since the owner of the photos confirmed that he only sent the photos to Prometheus, this solidifies the link between users Prometheus, Russian, and NSFW.

Argon: why did he send you his pictures
Russian: pictures?
Russian: that was ages ago
Russian: when i decided i was done with him
Russian: and he was useless
Russian: i social engineered him
Russian: and sent fake pictures of myself
Russian: and he trusted me and sent me his
Russian: and i also found out where he lived then
Russian: and where he worked and where he went to college

4.2.2.D

CONNECTING PHOTON TO PING AND CROOK

HELL RELOADED DATABASE

Tutsman, one of Hell Reloaded's former admins, was responsible for dumping the site's database and selling offering it for sale within private circles. The following screenshot shows the Hell Reloaded databases sold by Tutsman were dumped on February 18, 2016.

```
-- =====  
--  
-- Database dump of tables in `exodus2db`  
-- February 18, 2016, 06:41:08 pm  
--  
-- =====  
--  
-- Table structure for table `hell_admin_info_files`  
--
```

PRIVATE VERSIONS OF HELL RELOADED AND THEREALDEAL

A "private" copy of the Hell Reloaded and TheRealDeal databases were purchased directly from NSFW.

The purchased Hell Reloaded database was dated May 2016, and contains a significant amount of data removed from the copy currently being traded on the dark web (which is dated February 2016).

The copy of TheRealDeal forums was also purchased. In the SQL file, it contains a reference to the site's admins, Peace and Lava. Lava's email address is assemble@protonmail.ch, the same email used by Photon in the Oday introduction post.

```
INSERT INTO smf6_members VALUES('1', 'peace', 'peace@rows.io', '', '0', '0001  
INSERT INTO smf6_members VALUES('2', 'Lava', 'assemble@protonmail.ch', '', '0  
INSERT INTO smf6_members VALUES('3', 'TheRealDeal', 'trdtrd@mailinator.com',
```

PING BY ELIMINATION

As the known admin of both Hell forums and TheRealDeal forum, Ping would have access to both databases. Since both of the acquired databases have never been seen for sale, it would not be unreasonable to assume that Photon is an admin of both of these forums. Since Peace of Mind is attributed to a different threat actor (in the next section of this report), we can reasonably deduce that Photon (assemble@protonmail.ch) and Ping are the same person.

RUSSIAN ADMITS TO HACKING WORM.WS

During a private chat, Russian admits to hacking the w0rm.ws site by bribing a moderator. Based on the previous analysis of the leaked w0rm database, the "mod" is ke7hb.

Wait. Wtf. That means you hacked worm's site?

And w0rm was me yes

but that wasbecause i bribed a mod

WHO IS THE REAL PING?

A STORY OF DECEPTION AND MEDIA MANIPULATION

The user 'Ping' originally made news headlines as the admin of Hell forum. Prior to the forum's closing in 2016, a dox surfaced, implicating Dimitri Barbu of Calgary, Canada, as Ping.

The dox was published by users Revolt and CptCrnch, along with various screenshots and chat conversations that would appear to confirm their story.

Barbu was later arrested and charged with 39 counts of credit card skimming and card fraud.¹¹

Following his arrest, Barbu named Dionysios "Dennis" Karvounairis as the true Ping - a 15-year-old Calgary resident, and the person responsible for hacking the Calgary Board of Education (CBE) in order to access his school's TeacherLogic account.¹²

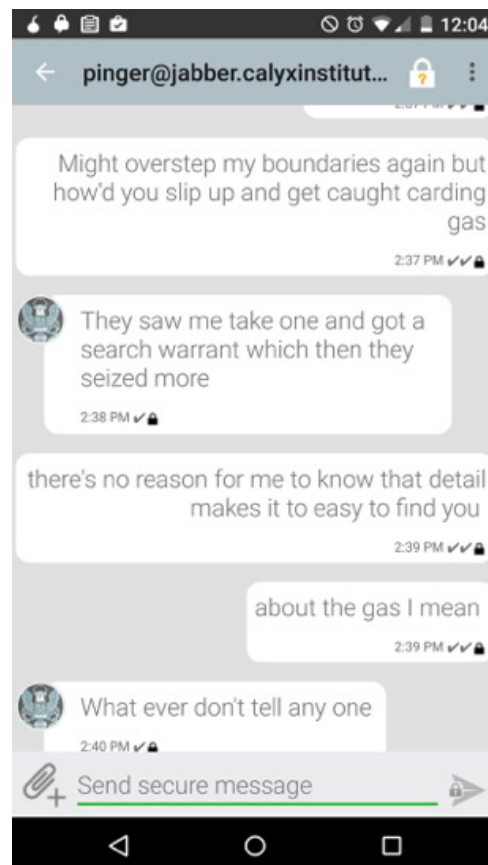
DK was subsequently arrested on suspicion of hacking.

Confirmation exists that the hacked TeacherLogic accounts were accessed from DK's neighbor's IP address, and that DK attended the school in question.

Following a search of DK's home, police discovered several devices and accounts using the username 'Ping', and a TOR hidden service called 'PingSec'.¹³

The dox of Barbu, sent directly to the media, included screenshots of private XMPP conversations between Pinger and Revolt as further evidence suggesting Dimitri was the real Ping.

More detailed information on this story is available in the book "Hunting Cyber Criminals".



¹¹ https://motherboard.vice.com/en_us/article/gv5dzq/the-administrator-of-the-dark-webs-infamous-hacking-market-the-real-deal-has

¹² <https://www.deepweb-sites.com/notorious-dark-web-hacking-forum-hell-run-canadian-teenager/>

¹³ https://motherboard.vice.com/en_us/article/ywmjav/canadian-teen-allegedly-behind-notorious-dark-web-hacking-forum

NSFW CONFIRMS THE IDENTIFY OF PING

The following XMPP conversation was sent to me by NSFW using the address BTC@richim.org. The conversation is between DK (whereami / Ping) and NSFW (who is CM, discussed in the next section).

In the following chat, NSFW intentionally reveals the identity of Ping. It is reasonable to conclude that these logs were sent to this researcher by NSFW as a means to incriminate his partner (DK).

```
whereami:    He knows I am Greek though
NSFW:       bro
NSFW:       when i type in
whereami:    Like fuck all these niggas getting arrested is adding up
NSFW:       "Dio_The_Plug"
NSFW:       it comes up with
NSFW:       https://twitter.com/CalgaryPolice/status/912750695559958539
NSFW:       on google
NSFW:       and yeah
whereami:    Bestbuy also snitched
whereami:    Dude only you know of that name
whereami:    Your not going to snitch to on me?
NSFW:       you need to get it removed from that somehow
NSFW:       listen
NSFW:       Im not after you
NSFW:       but
NSFW:       others are
whereami:    I did I deleted my twitter
```

The account "dio_the_plug", which has since been deleted from Twitter, was also used as Dennis' Instagram account. Searching the name will still link you to his former Instagram friends.

A google images search for that name will also lead you to the picture of DK in a sombrero shown on the next page.

4.2.3

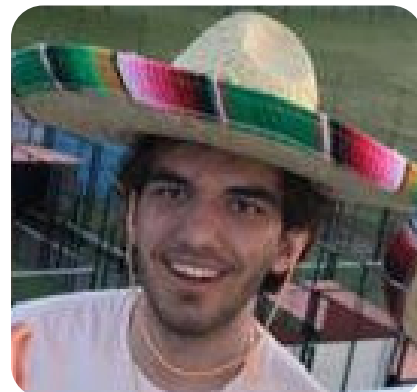
SUMMARY

A summary of user Cr00k and his association with DK

Evidence suggests that Dionysius "Dennis" Karvouniaris, 18, of Calgary Canada, is user cr00k and one of the original member of The Dark Overlord hacking group.

DK is an extremely gifted hacker, and even more gifted at the art of deception and operational security. His previous aliases include Photon and Ping, and was the original owner of Hell forum.

His most recent affiliation with NSFW puts him at the center of a number of high profile hacks, including being a member of the hacking group



KNOWN ALIASES

- c86x
- Columbine
- Cr00k
- Dio_the_plug
- F3ttywap
- Jinn
- Lava
- Malum
- Nakk3r
- NSFW (shared)
- Overflow
- Photon
- Ping
- ROR[RG]
- Russian
- Ryder



4.3

Name: Christopher Meunier (CM)

PEACE OF MIND

Age: 19 Location: Calgary, Canada

ALIASES

AmiEdgyEnough
Diablo
Frosty
Kolon
Mastercorp
Megadimarus
NSA
NSFW
Obfuscation
Omnichorus
Revolt
ROR[RG]
Soylent
Stradinatras
The_Dick_Head
Trickster
Vladimir
WhitePacket
ZLO

AFFILIATIONS

CanadaHQ
Hell
Gnostic Players
KickAss
NSFW
Shiny Hunters
TheRealDeal

JABBER IDS

btc@richim.org
columbine@xmpp.jp
frosty@digitalgangster.com
nsa@rows.io
obbylord@jabber.de
revolt@jabber.calyxinstitute.org
stradinatras@swissjabber.ch
thedarkoverlord@rows.io
whitepacket@xmpp.is

EMAILS

cash60617@sbcglobal.net
chris@whitepacket.com
chrismeunier@yahoo.com
chrstphrlngly@yahoo.com
extrememeunier@gmail.com
hackernike@live.ca
howtobashwindows@gmail.com
ihellg0d@live.com
jack.derpinstein@gmail.com
kayehkayeh@hotmail.com
pimp_alex91@hotmail.com
retrocops@hotmail.com
whitepacketweb@gmail.com

DOMAINS

Og.money
Whitepacket.com

SOCIAL MEDIA

facebook.com/PimpAlex91
twitter.com/whitepacket

PASSWORDS

1adgjmP*
s1swoc2nworb
brown2cows1s
Dicksquad1

4.3.1

ACTOR SUMMARY

CM's history of cyber-crime and credit card fraud has been traced as far back as 2014 under the names Stradinatras and Revolt. Despite his many aliases, CM's communication style is typically aggressive. He participates in bug bounties under the alias 'WhitePacket' and has his own cybersecurity company called White Packet security. It is believed that CM took over as leader of TheDarkOverlord in 2017.

Evidence suggests CM, also known as NSA, is the group's primary hacker. CM is believed to be responsible for the development of several paid botnets, hacking the Louisiana DMV, iMesh, and may be involved in the use and distribution of the Mirai Botnet. Evidence also suggests that CM is the owner and operator of CanadaHQ.at, a darkweb marketplace focused on Canadian-based crime.

A THEME OF SEXUAL ORIENTATION

CM is aggressive in his communication and references towards gay and homosexual behavior. He regularly refers to himself as a 'fag' on his personal Facebook page and used the word often to describe others. Subsequent sections of this report will show that similar language used throughout his online persona.



TACTICS AND PERSONALITY

CM's greatest strength is his ability to deceive and create confusion, which he does under the guise of multiple aliases. CM will often spend a significant amount of time engaging in confrontational conversations with himself under different aliases in order to create the illusion that he is not involved in the topic being discussed. Conversations with CM often have an aggressive undertone, and quickly become hostile. His mannerisms are easily distinguishable from others due to their aggressive and often gay-bashing nature.

ROLE IN TDO

CM was one of the core founding members of TDO under the alias NSA (nsa@rows.io). It is believed that CM took over leadership of the group in 2017, following their public announcement on Twitter. CM's role as leader of TDO corresponds with the group's increased level of aggression and hostility towards its victims, and includes more of an emphasis on terrorizing than actual hacking.

4.3.2

RELATIONSHIP WITH DK

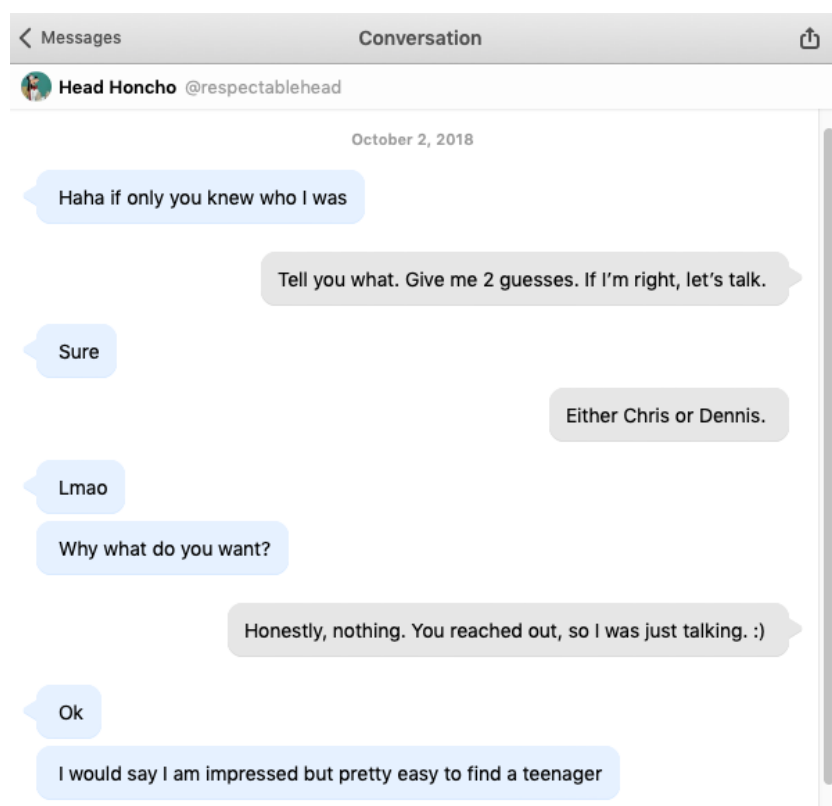
CM's history of hacking appears to originate with the alias "Revolt" which first appeared on Hell forum. The original Hell forum has since been confirmed by law enforcement to have been operated by DK.

DK and CM are lifelong friends who grew up living only a few miles from each other in Canada.

Individuals close to both CM and DK have even cited an instance where the two individuals were questioned by the Canadian authorities for sending stolen pizzas to people's homes that were purchased using stolen credit cards.

In addition to working together on hacks related to The Dark Overlord, it is believed this duo were the primary actors behind the name NSFW.

Subsequent sections of this report will show how the two threat actors conspired to manipulate mass media into associating the identity of 'Ping' with another common credit card thief from Calgary.



4.3.3

ATTRIBUTION

CONNECTING CM TO TDO AND OTHER ORGANIZATIONS

ATTRIBUTION SECTIONS

A. Revolt, WhitePacket, ZLO, and Vladimir

B. Peace of Mind and the W0rm Hack

C. Peace and TheRealDeal Market

D. NSA, Revolt, Orion, and Diablo

E. Connecting Orion and NSFW to TDO

F. Linking CM to Stradinatras and Obfuscation

4.3.3.A

REVOLT, WHITEPACKET, ZLO AND VLADIMIR

REVOLT

User Revolt first appeared on Hell forum in 2015. During his initial posts, Revolt appeared to be very young and new to hacking, learning as much as he could from his forum peers.

The friendship between Revolt and Ping was apparently strong, as Ping gave Revolt full control of Hell forum's private database repository.



ping

Don't mean to sound like a dick or anything but I just put revolt in charge of updating my server for me because I am busy. You guys do realize this server has been up for over a month and so far its only shit that I have uploaded.

ZLO PARTNERSHIP

Circa July, 2015, user Revolt introduces ZLO on Hell forum as part of a new partnership that was formed. ZLO posted the following message:

This is Zlo, the owner of ZIB Tor Botnet here on the dark web. Me and Hell have partnered up, and will be releasing the bot-net branded under Hell. We will have a board with a bugfix and suggestions section, and we'll be able to hold up a very nice piece of malware. Can I get some confirmation?

Download: The ZIB botnet is currently available as a free download on Whitepacket's Github page: <https://github.com/whitepacket/>

The following conversation with a former Hell forum moderator discusses ZLO (Whitepacket) also being an admin on the forum.

No the guy. He was a mod on hell

Oh no. Admins on hell that I knew we're me ping
revolt cypher whitepacket

Under what name ?

There was no whitepacket in hell

Nah he was when they wanted him to release his
botnet

CM ADMITS TO BEING ZLO AND VLADIMIR

In 2016, CM began speaking to tech reporter Bev Robb over Twitter regarding his association with Hell forum, and his volatile relationship with Ping.

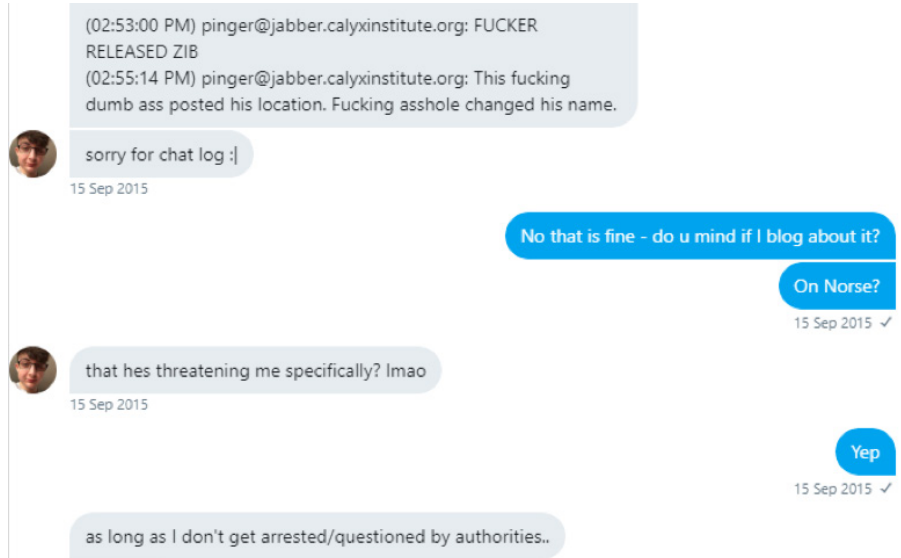
A number of private conversations occurred between WP and tech reporter Bev Rob. The following screenshot shows WP taking credit for writing the ZiB botnet and admits to being users “ZLo” and “Vladimir” on Hell forum.



WHITEPACKET THREATENED BY PING

During his conversation with tech reporter Bev Robb, WP tells a story of being threatened by Ping for publishing the source code to ZIB botnet on his personal GitHub page. WP stated that Ping ripped him off for \$10,000, which is why he published the code.

In the following private conversation with tech reporter Bev Robb, WP expresses concern over being threatened by Ping for releasing the ZIB botnet code on his personal GitHub, and went as far as to file a complaint with Alberta's RCMP.



CONFIRMING WP AS REVOLT

The following private confirmation between this researcher and a threat actor HA (aka zer0ing) confirms 'Revolt' as the person who was threatened by Ping for leaking his code.

V: fine. who was the kid that ping threatened him in real life? something about using the kid's exploits?

H: Revolt

V: NO WAY

H: Revolt

V: no kidding

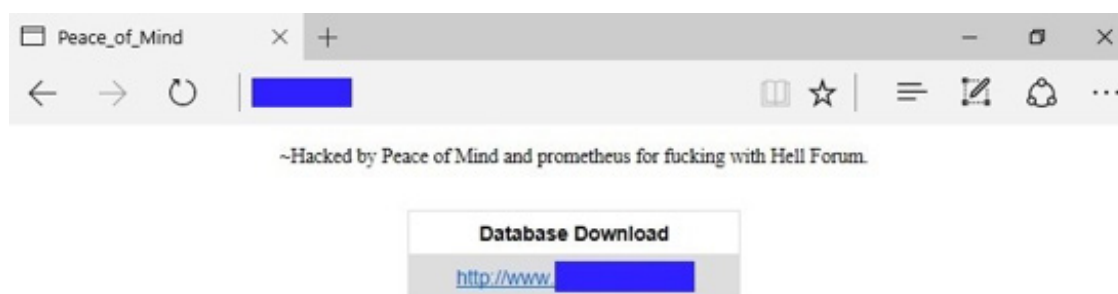
H: why would i do that

H: i still have their chat logs which revolt screenshot it

4.3.3.B

PEACE OF MIND AND THE WORM HACK

Information published on the hacked front page of w0rm.ws, a Russian hacking forum, directly attributes the site's hack with users Peace of Mind and Prometheus, for "f*ing with Hell Forum."



PARTNERS IN CRIME

The previous section of this report attributes Prometheus with DK, leaving an open question as to the identity of Peace of Mind. Given DK and CM's history of friendship and proclivity to hack and conspire together in the name of Hell forum, it would not be unreasonable to conclude that Prometheus' partner, Peace of Mind, is CM.

THE WORM HACK & KE7HB

Logs from leaked w0rm.ws forum dump show that user ke7hb ultimately transferred ownership of the forum to cr00k@swissjabber.ch.

Prior to the transfer of ownership (i.e., forum hack), ke7hb was a regular user on the forum. Several of ke7hb's private communications use the jabber ID data2z@swissjabber.org, which is also directly associated with TDO from their initial sale of data on forums Exploit.in and Bezlica.top.

```
(3049, 2508, 3048, 'ke7hb', 386, '', 1464451741, 'hi, I have contact for traffic \n [email] data2z@swissjabber.org [/email] is my temp jid.', 1, 0, '85.25.103.69', 0, 0, 0, 0, 0),
```

CONCLUSIONS

The chain of events surrounding the w0rm hack, and analysis of the forum's leaked data, indicate that that users data2z@swissjabber.org and cr00k@swissjabber.ch are two different people, both associated with The Dark Overlord.

4.3.3.C

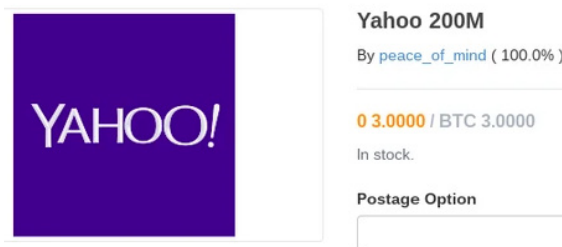
PEACE AND THEREALDEAL MARKET

WHO IS PEACE OF MIND?

Peace of Mind initially gained notoriety through the advertising and sale of several high profile data breaches including Yahoo, LinkedIn, MySpace, Tumblr, and more.

Each database was posted for sale on TheRealDeal (a darkweb marketplace), where Peace was also an admin.

In order to help promote the forum and the sale of his stolen merchandise, Peace agreed to be interviewed by Wired. In the article, Andy Greenberg writes,



*On an almost daily basis, new collections of data from hundreds of millions of stolen accounts have appeared on the dark web, ripped from major web firms and sold for as little as a few hundred dollars each worth of bitcoins. And behind each of those clearance sales has been one pseudonym: "Peace_of_mind."*¹⁴

THEREALDEAL MARKETPLACE

Owned by user Daniel Kaye (aka BestBuy aka Popopret), TheRealDeal became a central hub for the sale of Peace's stolen databases. TRD was also the central marketplace for users NSA and Arnie to sell data stolen by The Dark Overlord.

Note: In 2019, hacker Daniel Kaya, aka BestBuy, was sentenced to prison for operating the Mirai and GovRat botnets.¹⁵

A CONNECTION TO THE MIRAI BOTNET

Evidence from Kaye's seized equipment included Skype logs detailing conversations with two co-conspirators, one named **Chris** (presumably CM).¹⁶

The information is not related to The Dark Overlord, and therefore outside the scope of this report. The details surrounding this connection are available in our researcher's book, "Hunting Cyber Criminals".

¹⁴ <https://wired.com/2016/06/interview-hacker-probably-selling-password/>

¹⁵ <https://www.zdnet.com/article/hacker-bestbuy-sentenced-to-prison-for-operating-mirai-ddos-botnet/>

¹⁶ <https://www.zdnet.com/article/dutch-hacker-who-ddosed-the-bbc-and-yahoo-news-gets-no-jail-time/>

4.3.3.D

NSA, REVOLT, ORION AND DIABLO

The user alias NSA (nsa@rows.io), is associated with The Dark Overlord by way of several items posted for sale on TheRealDeal darkweb market, including the hacked Louisiana DMV database.

ORION

The following is an excerpt from a private conversation between a security researcher and ZeOring (aka Tutsman), another forum admin of the Hell Reloaded forum, in which he directly links Peace of Mind with Orion, the same person who was openly responsible for hacking Comcast in 2016.

```
ha: POM never had full yahoo i give him some samples and he posted it for sell
ha: orion is still around
v: who is orion?
ha: orion == POM
ha: his jabbers
ha: bx169@rows.io
v: wait
v: thats peace??
ha: yes
v: WOW
v: no shit
ha: ;)
ha: orion@securejabber.me
ha: comcast@jabber.calyxinstitute.org (POM)
```

ORION ON ODAY FORUM

During his application post on the Oday hacking forum, Orion introduces himself by offering a sample of his hacked Comcast database.



orion
November 02, 2015

Hey, looking for a new place to chill for a bit, also make money and share my knowledge. I have adminstarted a darknet hacking forum, drug marketplace and a couple of other small projects but thats in my past now for now i sell and/or trade dbs for example currently have comcast db 590k users with plain text passwords and some other high profile dbs. As proof here is a small sample of comcast. flennik@comcast.net:pinefern sfletcher1@comcast.net:jester23 sflew2s@comcast.net:l0cutus1 sflight1@comcast.net:fighters sflim@comcast.net:yinyee37 sflindgren@comcast.net:329723061 sflint14@comcast.net:soccer sflinx@comcast.net:05191990 sflitcraft@comcast.net:cheryl00 sflizm@comcast.net:fleming1 sflong@comcast.net:fortune sflowers3@comcast.net:50cent sfltodd@comcast.net:zappa

CONNECTING ORION TO NSA(@ROWS.IO)

Within the same application on Oday, Orion offers a link to his own personal collection of Exploit kits. The username for his collection is "nsa" and Orion even admits to putting up his own TOR services to host the files he assembled for the forum.

orion 
Account not Activated

Posts: 2
Joined: Nov 2015
Jabber:

Who invited you or how did you find us? long time ago i from a friend.

Post: #1

Your knowledge and skills? slqi,xss, other shit.

Why you want to be here? darkode is dead, no other place except for russian forums like maza and zeta.

what you will bring/share here? dbs,malware,source code,tools,shit like that.

Links to your profile on similar Tor/Cleartnet forums <http://darkode5vqwi4koz.onion/memberlist...file&u=140>

lol so we will stop there for now, i am not sure if he is le or just retarded anyways here is some free shit from me:

Link http://baddeath7lu7ioid.onion/Exploit_kit_collection.7z

User **nsa**

Password fuckthepolice

CONNECTING NSA TO REVOLT

Revolt's logo on Hell forum is Electronic Frontier Foundation (EFF)'s version of the National Security Agency logo, depicting an eagle with headphones (seen in the screenshot in Section 4.2.2E). *Revolt's version of the logo removes the AT&T logo from the center of the EFF logo.*



- User NSA on Hell Reloaded, O-day and SiphOn forums use the same avatar.
- User Revolt and NSA also share similar posts between forums.
- Both Revolt and NSA were moderators of Hell and Hell Reloaded (respectively).

VERBAL CONFIRMATION FROM NSFW

During a private conversation over jabber chat, actor NSFW (CM) links alias Revolt to himself, DK, and NSA (from TDO)

NSFW: bro revolt up till hell 2 Revolt was multiple people
NSFW: mainly me and ping and NSA from tdo

DIABLO & BX169@ROWS.IO

The following is a private message copied
NSFW's private Hell Reloaded database dump
between JohnSn0w and Diablo.

Diablo uses the jabber address bx169@rows.io,
previously connected to Peace of Mind.



JohnSn0w

February 02, 2016, 08:44:55
Hey man Jabber/ICQ?



Diablo

February 08, 2016, 06:15:49
bx169@rows.io

2016 COX COMMUNICATIONS HACK

In a forum post, Diablo admits to hacking
Cox Communications in 2016 and
provides the SQL vulnerability used in
the attack.

A few months later, user Malum (DK)
admits to having the data and posting it
for sale on TheRealDeal market.

Diablo

January 30, 2016, 00:06:41

hmm well I have given up on getting the passwords on cox employs, if any one can
help just drop it here please. Anyways what I have so far is everything about the
employs but passwords lmk if any one gets something good out of this.

```
[code]python sqlmap.py -u https://optix.cox.com/Louisiana/security/noaccess.asp?
id=chrgree&action=reset --random-agent --threads=10 --risk=3 --dbs[/code]
```

employ info is found in the table "security User" in the following dbs: "Optix_LA"
"Optix_PhX" etc.

malum

April 16, 2016, 17:09:12

We have the full dump.
We were selling it on RealDeal.
We shared the SQLi and anyone could have dumped anything previously.

U.S. GOVERNMENT HACKS

On March 27, 2016, user Diablo posts the following private message asking for assistance in cracking
password associated with a hack on GSA.gov and using them to organize more hacks against U.S.
government agencies.

*****DO NOT LEAK*****

I request help in cracking, password re use and SE, i give you the following data.

33k users - http://sumldjwuqdfh54vc.onion/HeLL_DataBin/US_Gov/users.csv

hashes - http://sumldjwuqdfh54vc.onion/HeLL_DataBin/US_Gov/Hashes

cracked hashes - http://sumldjwuqdfh54vc.onion/HeLL_DataBin/US_Gov/%24_1800.txt

...[List of agencies omitted]...

why am I sharing this? i got into gsa.gov emails i want to see how many more agencies we can get.

*For now i like for people to set up spear phishing attacks or just phishing as we have phone numbers
address and zip. SE is key here i think if you would like to talk more PM me.*

4.3.3.E

CONNECTING ORION AND NSFW TO TDO

In Section 4.2.2 of this report, evidence shows a chat log regarding the following photo sent from user Prometheus to user Ze0ring.

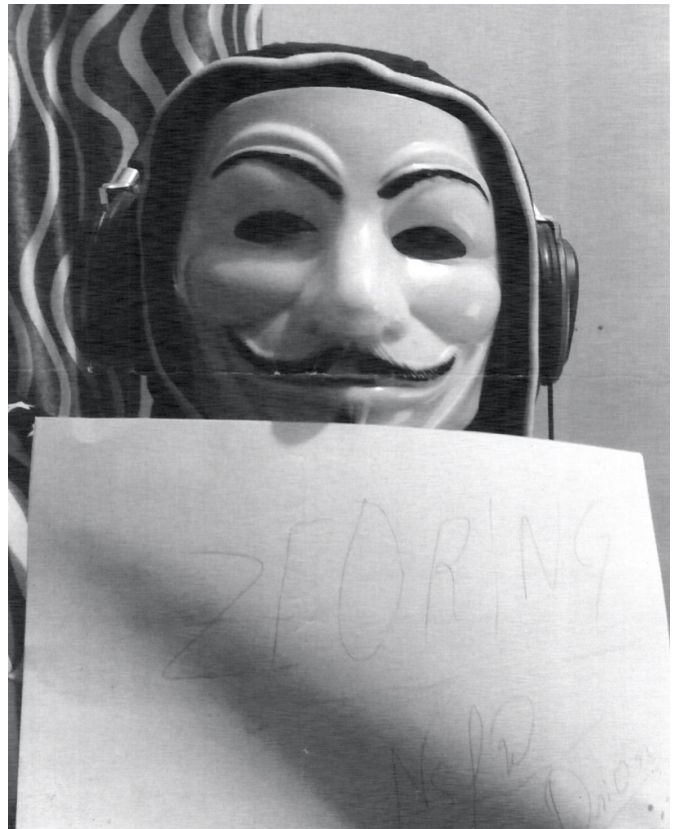
The photo, [REDACTED]

message for the recipient: NSFW / Orion.

In the private chat shown in the previous section, NSFW admits being sent the photo.

Finally, an email with [REDACTED]

[REDACTED] using a known TDO email address (confirmed in the Wyatt indictment).



* The hand-written message is written to NSFW / Orion

4.3.3.F

LINKING CM TO STRADINATRAS AND OBFUSCATION

The alias Stradinatras is primarily used on the carding forum Exploit.im. User Obfuscation (obbyLORD) is only seen on the KickAss forum. The following screenshots link the two users.

```
obbylord@jabber.de: can you send me logs on exploit?  
obbylord@jabber.de: user: stradinatras
```

```
obbylord@jabber.de: there is no stradinatras on KA  
obbylord@jabber.de: I am Obfuscation on KA, stradinatras on Exploit
```

A CONVERSATION WITH WHITEPACKET

The following is a direct conversation between this researcher and WhitePacket. During our brief conversation, CM made a reference to 'NightCat', an alias used on Exploit.im to communicate with a single person: Stradinatras.

```
whitepacket: are you in the law enforcement industry?  
Vinny Troia: no. and you can quickly see that by googling my name  
Vinny Troia: there's no money in being in LE  
whitepacket: I'm sorry man but you sound like you're either LE or a fucking retard, probably the  
latter.  
Vinny Troia: why am i a retard?  
whitepacket: you and your friends NightCat/jasonvoorhees/hafez asad and other dickheads can go  
climb a wall of dicks  
whitepacket: KickAss is a honeypot  
Vinny Troia: ok wait  
Vinny Troia: hafez i've heard of. he was banned from KA a while ago  
Vinny Troia: i saw a post that he worked for some agency  
Vinny Troia: i dont think KA is a honeypost, but that's def your opinion  
Vinny Troia: NightCat?  
Vinny Troia: jasonvoorhees  
Vinny Troia: ?  
whitepacket: s u c k a d i c k
```

Note: Orion used the same comment, "LE or a retard" in NSA's Oday application post.

4.3.4

SUMMARY

Summary of user NSA and his association to TDO

Christopher Meunier (CM), 19, of Calgary Canada is believed to be the individual behind the personas of several significant threat actors, including Peace of Mind, NSFW, Revolt, NSA, and The Dark Overlord.

Moonlighting as a legitimate cybersecurity company called WhitePacket Security, Meunier started hacking around the age of 14 under the alias Revolt.

The alias Peace of Mind is well known as a data broker in connection to the sale of very high profile data breaches on TheRealDeal market.

The alias NSA (nsa@rows.io) is believed to be responsible for hacking the Louisiana DMV, while CM used the alias Diablo to infiltrate Cox Communications and GSA.gov.



Following the formation of The Dark Overlord hacking group, it is believed that WP assisted with the selling of TDO medical data, and most likely assisted with leveraging the Xdedic 'RDP' server access to pivot to other medical victims.

In 2017, it is believed that WP took over as the sole persona behind The Dark Overlord, and is the reason behind the group's increased hostility and aggression towards its victims.

Evidence suggests WP was the head of The Dark Overlord during the violent attacks on the Iowa, Montana, Texas, and Alabama school districts, forcing school closings for as many as 5 days.

KNOWN ALIASES

- AmiEdgyEnough
- Diablo
- Frosty
- Kolon
- Megadimarus
- NSA
- NSFW
- Obfuscation
- Omnicorus
- Peace
- Peace of Mind
- Revolt
- ROR[RG]
- Soylent
- Stradinatras
- Trickster
- Vladimir
- WhitePacket



4.4

Name: Nathan Fyffe Wyatt (NW)

ARNIE

Age: 36 Location: Wellborough, England Phone: 44 775-481-6126, 337-214-5137

ALIASES

Arnie
CraftyCockney
Gingervitis
JasonVoorhees
I00t5
Mas
Mari0

SOCIAL MEDIA: <https://www.facebook.com/profile.php?id=100010064775327>

JABBER IDS

arnie@rows.io
gingervitis@wtfismyip.com
proter3@rows.io
thedarkoverlord@xmpp.jp
thedarkoverlord@rows.io

EMAILS

craftycockney@ymail.com
marco.weebler72@gmail.com
masbasher@gmail.com
masndave@gmail.com
thedarkoverlord@hotmail.com
thedarkoverlords@gmail.com

PASSWORDS

masmas12
3whores+1

HISTORY

Evidence suggests NW was involved with TDO at the onset of the group's formation in 2016. It is believed that Wyatt was the original persona of Arnie, intended to be the group's lead figure and patsy.

On September 24, 2016, NW was arrested on suspicion of Computer Misuse Act offenses for attempting to broker the sale of pictures of Pippa Middleton that were hacked from her iPhone.

In December 2016, following a search of NW's devices, the London Metropolitan Police Service found evidence of thousands of stolen documents from a UK law firm previously extorted by TDO.

Wyatt has been extradited to the United States on several charges related to crimes associated with The Dark Overlord group.

As of July 2020, Wyatt has agreed to plea guilty for his involvement in crimes related to The Dark Overlord group.

4.4.1

THE ORIGINAL "DARK OVERLORD"

ROLE IN TDO

Evidence suggests NW was involved with TDO at the onset of the group's formation in 2016. It is believed that Wyatt was one of the original personas behind the Dark Overlord, and also acted as the group's original lead figure under the alias Arnie.

In an interview with DataBreaches.net, Wyatt admits to "teaching thedarkoverlord fraud techniques", and was asked by a group member to "make an extortion phone call to a U.S. victim".¹⁷

It is our opinion that, NW was ultimately setup to take the fall for the group's crimes. This theory is supported by the fact that Wyatt allegedly opened bank accounts in both his and his girlfriend's name which were used to withdraw funds from TDO extortions.¹⁸



In an interview with DataBreaches.net, Wyatt was questioned regarding specific chat logs sent to law enforcement that appear to implicate him.¹⁷ When asked about what was in the chat logs, Wyatt responded,

"Him running details past me etc Its built in a way that it looks like i was tdo boss."

PRIVATE FACEBOOK CONVERSATION LOGS

Despite Wyatt's obvious need to deny any involvement with TDO, personal conversations with him show a very clear understanding of how the group operates. The following is a screenshot from a Facebook conversation between Wyatt and another party.

In conversations on the next page, Wyatt never comes out and states that he was a part of the group, however, he does admit to knowing the people and working with a single person ("a kid"), and a potential third person that helped with language and grammar.

Nathan Fyffe Wyatt

Tdo got in everywhere via xded... it's only that what was inside the rdp the security was so lax... the rest is history

Oct 27, 2019, 8:51 AM

Evidence suggests the "kid" is NSA (CM), and the third person is Cr00k (DK).

¹⁷ <https://www.databreaches.net/what-opsec-member-of-thedarkoverlord...accounts/>

¹⁸ <https://www.dailymail.co.uk/news/article-6578213/Stay-home-father-accused-hacking-fights-extradition-US.html>

4.4.2

CONVERSATIONS WITH WYATT

The following are snippets of conversations between Wyatt and a redacted third party.
Only Wyatt's statements are included.

REGARDING THE XDEDIC MARKETPLACE

Yeh I was a member... they had an rep in everyone zip code or postcode area code you wanted
You could buy an rdp from 2 to 15 bux... you knew where it was who's it was...
It took no intellect mate... just knowledge & membership of the marketplace
Tdo got in everywhere via xded...
it's only that what was inside the rdp the security was so lax... the rest is history

REGARDING TDO'S NEW LEADERSHIP

Theres wasnt a handover.... the story was he was too scared to carry on...
my last comm with him was when I had been arrested and then bailed
the kid I knew... the kid in those surgerys... I was always bro or homey .. didnt even use our users..
It was like chatting to a bro... he was inexperienced lookin to learn..
Although some of the details and language he would use in the comms with the CEOs wasn't they
kid I spent hundreds of hours with
Someone had prettied that up alot.
Almost someone who had really good grammar and vocabulary..


REGARDING THE IDENTITY OF TDO'S NEW LEADER

Reputation..professionalism ... the tdo I know... **would spaz out make threats be aggressive**
I dont know anyone name...what I say wont get anyone arrested... in all reality itll be info they
should know that maybe is just unsolved so to speak

4.4.3

A PERSONAL CONNECTION TO CM?

Around June 2016, a post was created on KickAss regarding the sale of TDO's medical data. User I00t5 vouches for the sale of TDO's medical data. Obfuscation (CM) outs I00t5 as being Arnie. L00t5 instead refers to himself as "Bill".




cr00k
Banned

I00t5 Wrote: →

Ooo very nice. I know this guy! vouch for seller if anybody's interested

Pretty sure more than 1 person knows him, he gets greedy easily, he will never find a buyer for these prices.



I00t5

Yes, price is high. but this price is for buy all fresh DBs, and only so high for public advertisement. Interesting move. DB also include dea#s and pii of doctor and insurance informations of patient. seller part db out and price is negotiable. All depend on your method for use this informations 😊


(edit by [Obfuscation](#))

He's a super greedy person, hard to deal with and stubborn.

Also enjoys the spotlight a bit too much.

Plenty of DBs get hacked every day, his is nothing special. He should just bulk the CVVs instead of selling shit 100s at a time and end up killing his base, which he already did by mediatizing his hacks.

Oh well, I guess he will learn.



Obfuscation
Trusted Seller
★★★★★

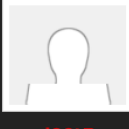
Posts: 760
Threads: 86
Reputation: **47**

Yes I agree with comment of selling small batch of cvv. This is all it take for kill a whole base.

Mediatizing hack is not so much of bad idea if goal is for sell. Anybody can buy now with such open source attention- nation state etc. If seller release name of base it does not matter. Maybe only to carder lol

Wellpoint/ Anthem breach 2014 is good example. Everybody know breach happen, all customers are warned, and credit-repair service offered... lol... this is only mitigation for small minded methods. If you think about the informations this database contain, then you can see what other values this have...

..




I00t5
Banned
failed!

I00t5 Wrote: →

Mediatizing hack is not so much of bad idea if goal is for sell. Anybody can buy now with such open source attention- nation state etc. If seller release name of base it does not matter. Maybe only to carder lol

Wellpoint/ Anthem breach 2014 is good example. Everybody know breach happen, all customers are warned, and credit-repair service offered... lol... this is only mitigation for small minded methods. If you think about the informations this database contain, then you can see what other values this have...

Sounds to me like you are Arnie.




Obfuscation
Trusted Seller
★★★★★

Posts: 760
Threads: 86
Reputation: **47**
Level: 25 [🔥🔥🔥]
Total Points: 3,964

Obfuscation Wrote: →

Sounds to me like you are Arnie.

LOL no detective, I am Bill.



I00t5
Banned
failed!

I00t5 Wrote: →

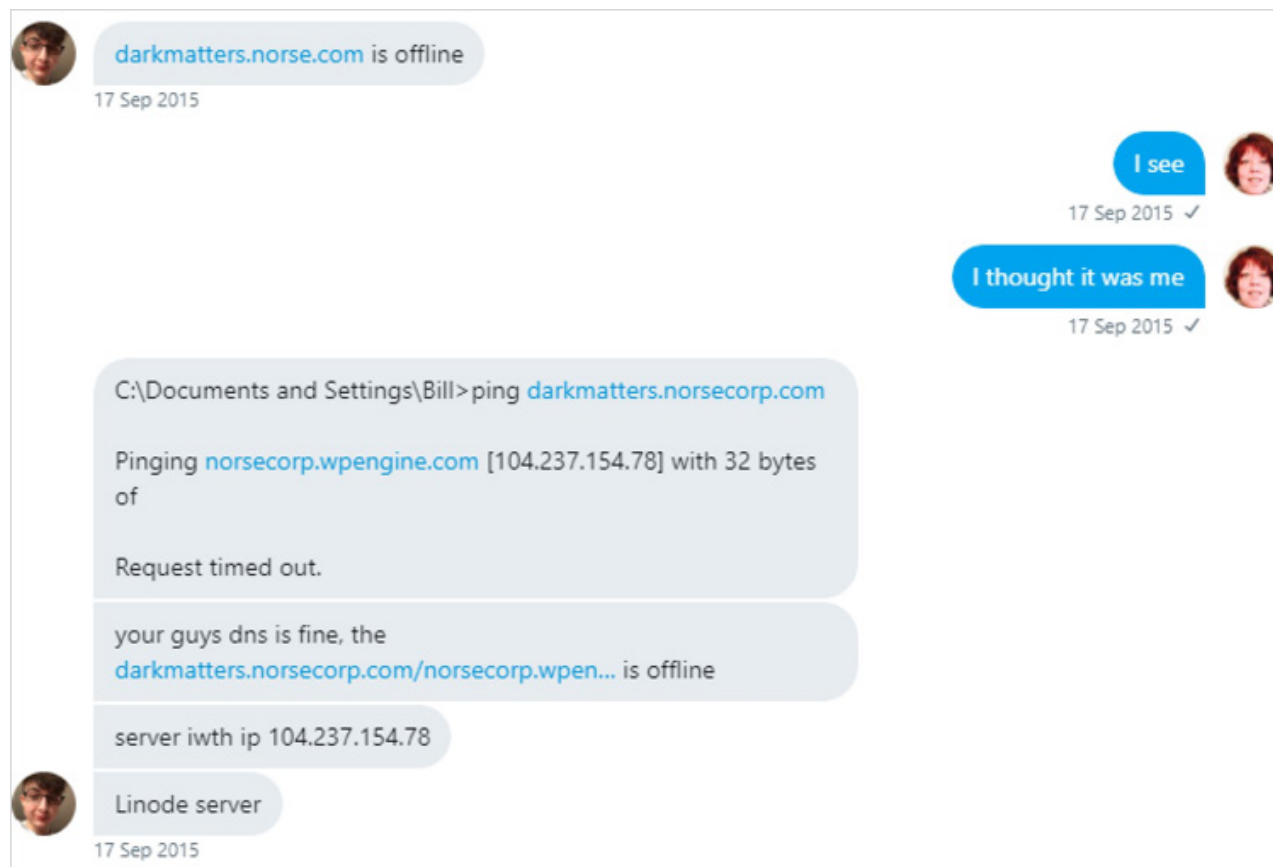
Sounds to me like you are Arnie.

LOL no detective, I am Bill.

4.4.4

WHO IS BILL?

As it turns out, William "Bill" Meunier, is CM's father. In private conversations with Bev Robb over Twitter, CM sends Robb a paste of his windows terminal. The username on the computer is Bill.



In other conversations shared with Robb, WP discusses using Pidgin on his father's PC to communicate with other threat actors.

ANALYSIS AND THEORY

In other conversations, CM refers to using his father's computer when logging onto XMPP. It is our theory that user Obfuscation (CM) knew I00t5 was Arnie. Sources close to both actors state the turmoil between the actors. This turmoil (and possibly NW's arrest) marks the transition of leadership to CM (TDO 2).

Arnie (I00t5), having a history with CM, could have easily known Bill to be CM's father's name. It is possible he also saw similar screenshots and thought CM's name was Bill.

When CM outed I00t5 on KickAss as being Arnie, I00t5 shot back with the name he could associate to his former partner.

4.4.5

INDICTMENT AND EXTRADITION

Nathan Wyatt, a 38 year-old man from Wellingborough who is also known as “Crafty Cockney,” has been extradited to the United States, facing six counts in an indictment issued by a grand jury in the Eastern District of Missouri:

One count of conspiracy against the U.S. (18 USC 371); Two counts of aggravated identity theft (18 USC 1028); Three counts of threatening damage to a protected computer (18 USC 1030).

The following supporting information was obtained from the official court documents:



- *Victim funds were transferred to a PayPal account with email tashiadsmith@tutanota.com*
- *Threatening extortion text messages were sent from 337-214-5137, which was registered using Wyatt's home IP address*
- *Wyatt registered a Whatsapp account with 337-214-5137 and uploaded his photo as the avatar*
- *The same number was used to log into the PayPal account that received the victim payments, and was setup as the home phone for that account*
- *An extortion email sent to a victim requested funds be split into four different UK bank accounts. The emails included bank account information in Wyatt's name and his girlfriend's name.*
- *A UK number 44 775-481-6126 was registered to Nathan Fyffe. That number was used to register Wyatt's personal Facebook account, and the @TDOHACK3R twitter account used by the group.*
- *The same phone number was used to order pizza for home delivery to Wyatt's home address, and was also used to register a VPN service that was used to log into the above TDO accounts.*
- *According to records recieved by Google, Wyatt's home IP connected to several TDO email accounts.*



Section 5

The Dark Overlord

Other Affiliations

NSFW

Evidence suggests CM is the primary persona behind the alias NSFW, but at one point was also shared by both DK and CM. Distinguishing between the NSFW aliases can be difficult as we can show instances where the two actors share chat logs in order to ensure consistent communication in their business dealings.

ALIASES AND COMMUNICATION

Our direct communications with NSFW occurred using the following jabber accounts:

- columbine@xmpp.su (CM)
- btc@richim.org (CM)
- nsfw@jabber.se (CM)
- nsfwisafed@jabber.ua (DK)
- russian@xmpp.is (DK)

During our experience purchasing data from "NSFW", one member would provide the data while another would receive the funds. In addition, two or three of the above accounts would log-on and off at exactly the same time to give a unified appearance.

```

nsfwisafed:    Also "AmlEdgyEnough" is not me
nsfwisafed:    As well as BTC@richim, he used that more than me
nsfwisafed:    BTC isn't me
nsfwisafed:    BTC@richim and BTC@xmpp.is
V:             But BTC came from NSFW
V:             also Photon gives both as him
V:             nsfw@ and russian@
nsfwisafed:    yeah, its on purpose
  
```

VICTIM LIST

The following hacks and data breaches can be attributed to the group NSFW:

- | | | |
|---------------------|---|---------------------------|
| • Army Force Online | • Flipboard | • PolyCount |
| • Bell Canada | • GSMA Intelligence | • RedBull Sound Select |
| • BotOfLegends | • Linux Mint | • Sephora |
| • Carding Mafia | • Foodera | • TeamSkeet |
| • CodeChef | • FrontLineSMS | • Timehop |
| • Comcast | • Lead 411 | • Tokopedia |
| • Datalot | • LifeSafer / LMG Holdings | • Turkish National Police |
| • DoorDash | • LivSpace | • University of Phoenix |
| • DotaHut | • Massachusetts Institute of Technology (MIT) | • Voxy |
| • FemaleDaily | • MGM Grand International | • Zoomcar |
| • Filmow | • MPGH | |
| • FiveStars | | |

5.2

GNOSTIC PLAYERS

Gnostic Players is a group of primarily French hackers that made their debut in 2019 with a 6-part sale of data breaches totaling more than 2 billion compromised records.

Three of the group's members were arrested in December, 2019 following the group leader's public admission to the hack of GitHub, and the group's theft of 10 million dollars worth of XRP.

GROUP MEMBERS

Name	Aliases	Role
Gabriel Bildstein	Nclay, OutofReach, Kuroi'SH, Snoupinet	Patsy / Public figurehead
Maxime Thalet-Fischer	DDB, Casper, RawData, Pumpkin	Seller
Nassim Benhaddou	Prosox	Member
Christopher Meunier	Omnichorus, Peace, Revolt, Whitepacket	Hacker
Dennis Karvouniaris	Ping, Photon, Russian	Seller / Hacker

VICTIM LIST

- 500px
- 8fit
- 8tracks
- Animoto
- Armor Games
- Artsy
- Avito
- BlankMediaGames
- Bookmate
- Bukalapak
- Canva
- Chegg
- CoffeeMeetsBagel
- Coinmama
- Coubic
- DailyBooth
- DataCamp
- DubSmash
- Edmodo
- Epic Games (Fortnite)
- Evite
- EyeEm
- Fotolog
- GameSalad
- GitHub
- Ge.tt
- GfyCat
- HauteLook
- Houzz
- iCracked
- Ixigo
- Legendas.tv
- LifeBear
- Live Journal
- LovePlanet
- mefeedia
- MindJolt
- MyFitnessPal
- MyHeritage
- MyVestigage
- Netlog & Twoo
- OMGPop
- Onebip
- Overblog
- Petflow
- PiZap
- PromoFarma
- RoadTrippers
- Roll20
- ShareThis
- Shein
- Singlesnet
- Storenvy
- StoryBird
- StreetEasy
- Stronghold Kingdoms
- Taringa
- Wanelo
- WhitePages
- Wirecard
- Yanolja
- Yatra
- YouNow
- Youthmanual
- Zomato
- Zynga

5.2.1

GNOSTIC PLAYERS & THE STORY OF GABRIEL: THE ULTIMATE PATSY

Gabriel Bildstein, aka Nclay, is another in a long line of patsies strategically put in place to take any attention away from the real hackers.

When speaking with Gabriel, it becomes immediately clear that he does not possess the technical knowledge needed to have carried out the group's attacks. Despite his lack of technical knowledge, his position is that he is/was solely responsible for hacking all of the sites associated with the group.

What makes Gabriel truly unique is his understanding of French law. According to his own admission, he knows that French law will not allow the extradition of its own citizens to the United States.

Therefore, any charges brought by the U.S. would need to be tried in French courts, which he believes will never happen because of his "mental condition".

This makes Gabriel the perfect scapegoat for any and all crimes. Gabriel firmly believes this, and continues to assume responsibility for all of the group's hacks.

He further believes that once people realize he does not have the technical skill needed to pull off the hacks, he will be released of all charges (because he did nothing wrong) and the real criminals, his "friends", will walk away free.



See Roman Polanski the rapist

He is wanted by the Us

And in France

He is not prosecuted

I know I didn't hack zynga and you know it too

So why would I need to tell the full story ?

To fuck up more lives ? No need

I am not going to tell it because I admitted everything to protect someone

I knew I had to confess

For the github hack

I was sure I was going to be released and that person was special to me

I didn't want this person to spend long time in prison

Happy with my answer ? You are welcome vinny

I won't I will face everything for the person I am trying to protect (NSFW)

If you want the truth about Dark Overlord

His real identity is sheissepacket

Whitepacket he is from Canada

5.3

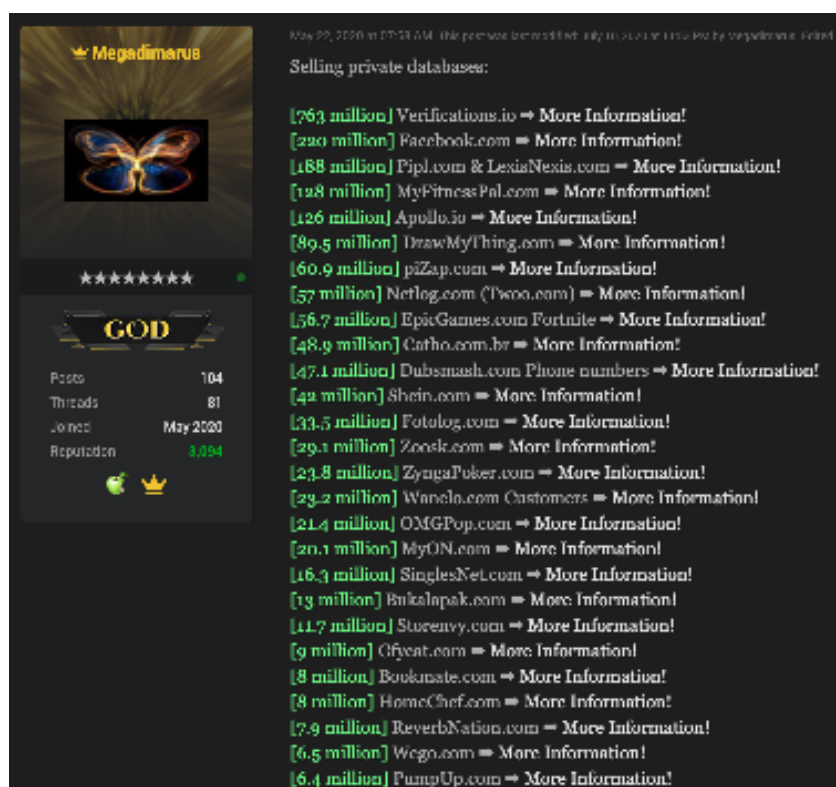
SHINY HUNTERS

In 2020, a new group emerged with the news of a 90 million user data breach of Indonesian firm Tokopedia. Shortly after the announcement, a slew of other data breaches followed, with promises by "Shiny Hunters" that more breaches would continue following in "stages".

ENTER MEGADIMARUS

Following the end of Gnostic Player (triggered by Gabriel's public admission for his crimes related to the GateHub hack), the group's primary seller, Omnichorus, mysteriously disappeared.

Thus, with the appearance of Shiny Hunters came a new seller, Megadimarus, who just happened to be selling all of Gnostic's old databases alongside the new Shiny Hunters databases.



Nov 29, 2020 at 07:33 AM. This post was automatically fully disclosed by Signal Messenger. Contact us for more information.

Megadimarus

★★★★★★

GOD

Posts: 104
Threads: 81
Joined: May 2020
Reputation: 3,094

Selling private databases:

- [763 million] Verifications.io → More Information!
- [220 million] Facebook.com → More Information!
- [188 million] Pipl.com & LexisNexis.com → More Information!
- [128 million] MyFitnessPal.com → More Information!
- [126 million] Apollo.io → More Information!
- [89.5 million] DrawMyThing.com → More Information!
- [60.9 million] piZap.com → More Information!
- [57 million] Netlog.com (Poco.com) → More Information!
- [56.7 million] EpicGames.com Fortnite → More Information!
- [48.9 million] Catho.com.br → More Information!
- [47.1 million] Dubsmash.com Phone numbers → More Information!
- [42 million] Shein.com → More Information!
- [33.5 million] Fotolog.com → More Information!
- [29.1 million] Zoosk.com → More Information!
- [23.8 million] ZyngaPoker.com → More Information!
- [23.2 million] Wanelo.com Customers → More Information!
- [21.4 million] OMGPop.com → More Information!
- [20.1 million] MyON.com → More Information!
- [16.3 million] SinglesNet.com → More Information!
- [13 million] Bukalapak.com → More Information!
- [11.7 million] Storenvy.com → More Information!
- [9 million] Gfycat.com → More Information!
- [8 million] Bookmate.com → More Information!
- [8 million] HomeChef.com → More Information!
- [7.9 million] ReverbNation.com → More Information!
- [6.5 million] Wego.com → More Information!
- [6.4 million] PumpUp.com → More Information!

VICTIM LIST

- Accuradio.com
- AT&T - 3rd party partner
- Catho.com
- Chronicle.com
- DrawMyThing.com
- Fluke.com
- Leafly
- Mathway
- Microsoft
- Minted.com
- Omlette.com.br
- PlayWings.co.kr
- Startribune.com
- Tokopedia
- Unacademy
- Wappalyzer
- Wego
- Wishbone
- Zoomcar
- Zoosk
- Zynga Poker

5.3.1

WHO HACKED TOKOPEDIA?

Shiny Hunters initially claimed ownership of the Tokopedia hack, using it to launch their new media spotlight. However, evidence suggests otherwise. In reality, Shiny Hunters, much like Arnie, or Nclay, is just another name in a long line of aliases designed to take attention away from the real hackers.

The hack of Tokopedia, was actually presented to us much earlier by user Russian (DK).

June 03, 2019

Russian: for poshmark
Russian: i had to wait a long time
Russian: like with timehop
Russian: and like with flipboard
Russian: and tokopedia
Russian: all these require waiting
Russian: waiting for a mistake
Russian: but now
Russian: poshmark
Russian: i lost all my access
Russian: some weeks ago
Russian: after i told u

WHO IS PLAYING THE ROLE OF SHINY HUNTERS?

According to our Gabriel, it's his buddy Prosox

outofreach@jabber.ua: Imma do a confidence
outofreach@jabber.ua: behind shinyhunters it's Nassim / Prosox
xxx: i thought it was you at first
xxx: i think shiny and mega are same person tho
outofreach@jabber.ua: shiny to take spotlight
outofreach@jabber.ua: no it's prosox

The focus of this report is not Prosox, so we will not be providing additional evidence to support Gabriel's claim.

5.4

CONNECTING ALL THE PIECES

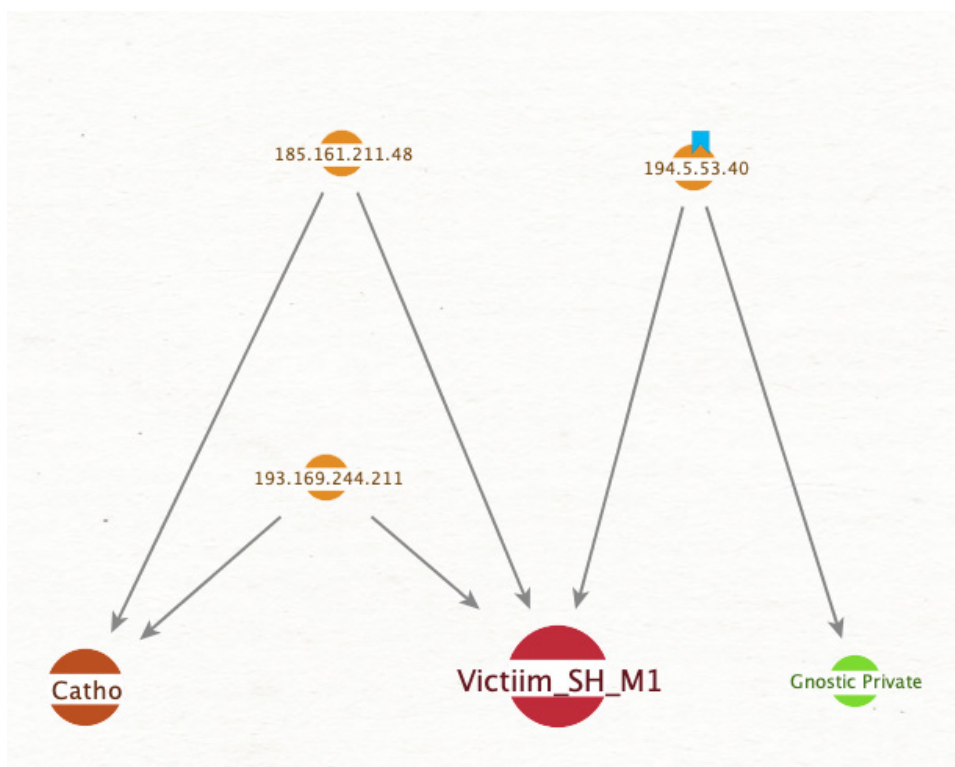
The evidence needed to connect each of the groups was provided by their victims.

After being in contact with at least twenty different victims, a clear pattern began to emerge when mapping the IP addresses used in their attacks.

According to the actors in question, they have no association to any of the other groups. For example, Nclay claims he is solely responsible for his own hacks, as does Shiny Hunters.

THE FIRST CONNECTION

The following chart shows a single connection between an IP used to attack a Shiny Hunters victim (in red) and an IP used to attack a Gnostic Players victim (in green). These attacks occurred more than two full years apart.



5.4.1

CONNECTING NSFW, GHOSTIC, AND SHINY HUNTERS

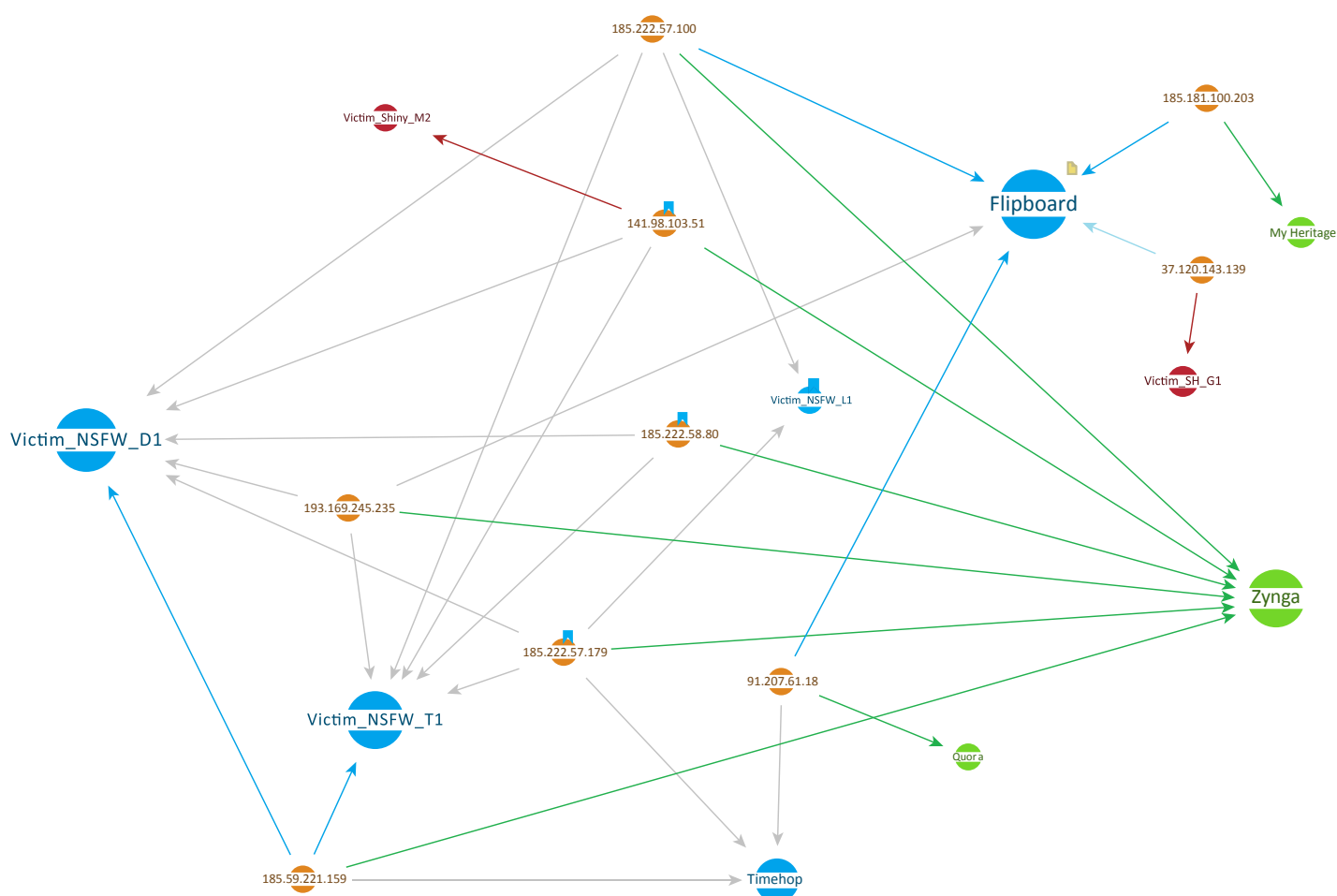
The following chart shows attacking IP addresses that correspond with color-coded Victims.

- Blue: NSFW victims
- Green: Gnostic Players
- Red: Shiny Hunters victims

While this chart may seem a bit overwhelming, the idea is that each IP address should only have one associated target (color) connected to it.

The IPs in this list are associated with overseas VPS accounts and are re-used over a multi-year period, spanning multiple victims and groups.

Some of the attack servers, such as 141.98.103.xx can be seen across all three groups over a 2-3 year period.



5.4.2

THE DATA VIPER "HACK"

As indicated in Brian Krebs' article,¹⁶ the data surrounding the hack of Data Viper turned out to be an elaborate hoax intended to discredit this report. We will be providing detailed evidence to support this fact in a forthcoming blog post.

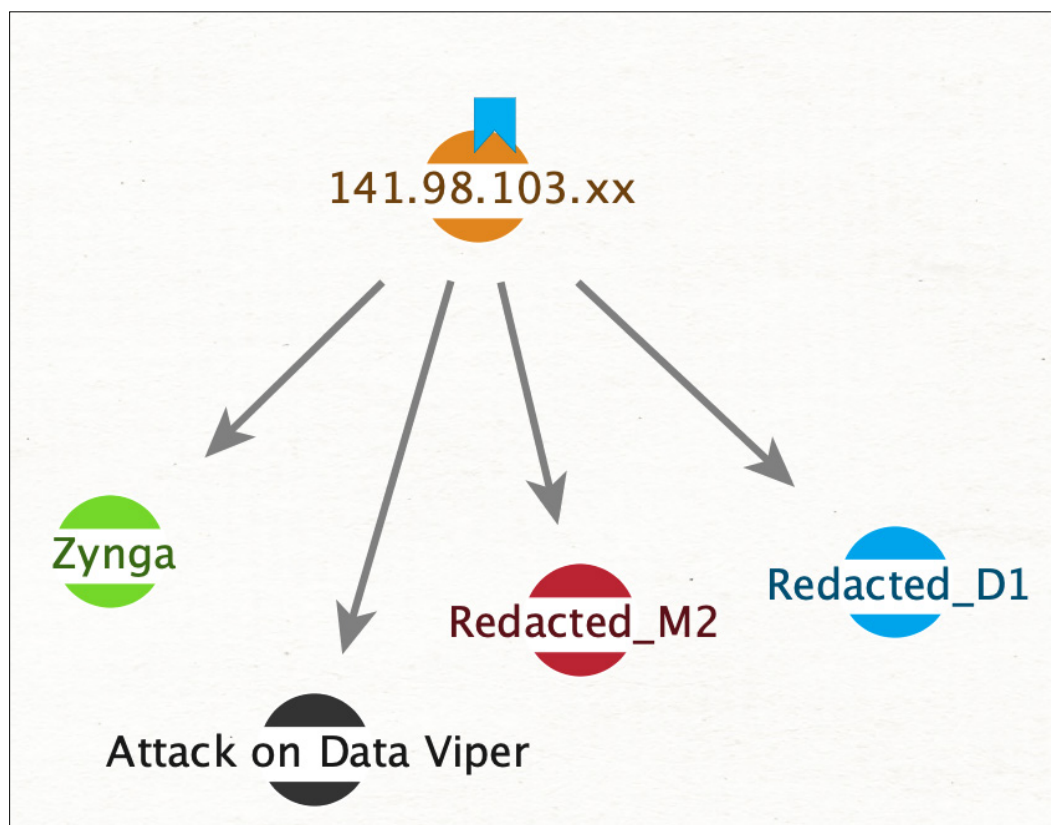
In reality, the "hack" was carefully orchestrated by our threat teams as means to draw out the attackers, who then used their staged victory to boast about their accomplishments to the media.

Revenge is mine, saith a hacker.

📅 JULY 12, 2020 👤 DISSENT

HOOK, LINE, AND SINKER

The same IP address used to access the Data Viper servers can also be seen accessing victims of Gnostic Players, NSFW, and Shiny Hunters, thereby confirming the connection between the groups and their members while also confirming who was behind the attempts to discredit this report.



¹⁶ <https://krebsonsecurity.com/2020/07/breached-data-indexer-data-viper-hacked/>



Section A
The Dark Overlord

Appendix

TIMELINE SUMMARY

2019

- TDO releases stolen information related to 9/11 attacks
- Nathan Wyatt extradited to the U.S. for crimes related to TDO
- Authorities shut down XDedic marketplace
- KickAss forum closes in exit scam; fakes seizure notice and changes URL
- Gnostic Players data on sale totals in billions of records
- Gabriel admits to hacking Gatehub. 3 members of Gnostic in France are arrested.

2018

- TDO re-surfaces. Begins campaign to promote data sale on KickAss forum
- TDO recycles hacked data - most likely attempting to rebuild lost BTC value
- Gnostic Players take focus

2017

- Wyatt makes YouTube recording of TDO extortion call
- Nathan Wyatt (Arnie) sentenced to 3 years
- TDO changes leadership - now run by Revolt / NSA@rows.io
- TDO targets students in Columbia Falls, Montana, and other school districts

2016

- Hell Reloaded, KickAss, and TheRealDeal marketplace launches
- Arnie and cr00k post medical data for sale on forums
- TDO accesses major healthcare organizations via RDP
- TDO gains access to additional orgs through HL-7 software
- W0rm rips off cr00k - cr00k dumps w0rm forum db
- TheRealDeal marketplace shuts down - \$2million+ exit scam

2015

- Revolt, Ping, and Cyper are active members of Hell Forum
- Revolt and CptCrnch dox Dimitry Barbu - claim he is Hell admin, Ping
- Dimitri Barbu arrested and names minor (DK) as person behind Ping alias
- DK questioned by authorities. PingSec server confiscated
- Hell shuts down

A.2

A LATE NIGHT CONVERSATION WITH TDO

The following text is a small portion of the almost 4-hour conversation that occurred on October 21, 2018 between TDO (believed to be CM) and Vinny Troia.

TDO: You're fortunate, tonight.

TDO: I'm sitting here moving terabytes of data into a new server, and I'm bored, so you've been blessed with communicating with me.

TDO: Your NSA and GCHQ is not as good as they want people to believe. Passive surveillance is only so successful.

V: i dont doubt that

TDO: Do you realise that we closed down six different school districts in Montana for 5 business days?

TDO: We closed out 36.000 students from school.

TDO: Now we've all heard about 'bombthreats' closing schools for a day, but what does someone have to do to close schools for 5 days?

TDO: Have you ever thought about this?

V: honesly, no

TDO: You're an idiot then. What other organisations have closed an entire region for that long?

TDO: Think about it. What did we need to do to achieve this goal?

TDO: 5 days. Not 1, but 5.v

TDO: Ponder it. We actually had your FBI physically chasing us,

TDO: Chasing ghost.s

V: I didnt realize the schools were closed for an entire week. You are right, that is pretty significant

TDO: You should read into it. It's all OSINT.

V: refresh me on the story, you guys were calling the school, correct?

TDO: Calling? Far beyond that.

TDO: We planted physical devices using unassuming third-parties.

V: i have no idea what that means

TDO: Fucking moron.

TDO: Think.

TDO: Use that fucking bit of grey matter between your eyes.

V: what is an unassuming third party
TDO: This is why your NSA and CIA investigated us, and conducted raids in London.
TDO: Mind you, unsuccessful raids.
V: I did not know anyplace was raided.
TDO: READ THE BILLINGS GAZETTE, the great piece of OSINT on TDO EVER.
TDO: Fucking moron, Troia.
V: let me ask you a question
TDO: Fuck, I'm sitting here on this evening speaking with the biggest moron on this fucking rock.
V: see, and i was about to offer you something really ice
V: nice
TDO: Fucking offer it, stop wasting time.
TDO: I'm fucking pissed right now, and horny enough to listen to the gay shit you spew out.
V: why are you mad?
TDO: I'm frustrated at how slow you are.
TDO: https://billingsgazette.com/news/local/after-columbia-falls-hack-that-closed-schools-experts-call-for/article_e3a8584e-cd15-5f19-a4e0-37bc2dbb2a1c.html
V: yeah im trying to read and talk to you at the same time
TDO: Speed up, mate.
V: I signed a book deal for OSINT. the book has a number of featured industry experts that are offering a tip or suggestion for a way they do things that is unique. Would you like to be a guest contributor? It would interesting to have something from someone on the blackhat side
TDO: What the fuck?
TDO: You want us to divulge TTPs for your fucking gay book?
TDO: You're so profit motivated it makes me fucking hard as fuck, mate.
V: It's weird you are finding this erotic
V: but yes, it would be a section in my book. pick a topic.
TDO: You're stoking my ego cock pretty good right now, so go on.
V: whats up with that 7 page ransom note? wasnt that a bit excessive?
TDO: Ah, I see.
TDO: What do you think
V: i think it was a bit excessive
TDO: Why?
V: just long i guess
V: could have summed it up in a few paragraphs
TDO: Do you realise that is our standard template?
V: oh. no i did not
TDO: We are verbose and condescending, quoted by the FBI.

A.3

HUNTING CYBER CRIMINALS

If you enjoyed this report, please consider purchasing a copy of Vinny Troia's new book, Hunting Cyber Criminals.

Hunting Cyber Criminals contains a mix of the technical tools and investigative processes and techniques used to uncover The Dark Overlord.

The book contains a number of personal stories, investigative road blocks, and Troia's own thought processes that led to the discovery of the group members.

Hunting Cyber Criminals will be available December 1, 2019 at Amazon and all other digital and physical book retailers.



Data Viper is the beginning of a new wave in cybercrime intelligence. Providing both real-time adversary threat intelligence and exposed credential monitoring for companies of all sizes. Data Viper was the sole threat intelligence tool used for this investigation.

For more information, visit www.dataviper.io

A.4

BREACH STATISTICS

The following breach statistics were used in the calculation of the figured listed in this report. Records breached are in millions of records breached.

Company	Year	Records Breached (m)	Source
2017 ITRC Cumulative	2017	16	ITRC
2017 Other	2017	140	HIBP / Leak-Lookup
8tracks	2017	18	Gnostic
Coinmama	2017	0	Gnostic
Dun & Bradstreet	2017	34	Other
Edmodo	2017	77	Gnostic
Equifax	2017	110	Other
Ge.tt	2017	2	Gnostic
Live Journal	2017	33	Gnostic
MyHeritage	2017	92	Gnostic
Onebip	2017	3	Gnostic
Petflow	2017	1	Gnostic
River City Media	2017	393	Researchers
Taringa	2017	27	Gnostic
Uber	2017	57	Other
Youku	2017	100	Other
Younow	2017	41	Gnostic
Zomato	2017	17	Gnostic

Company	Year	Records (m)	Source
2018 ITRC Cumulative	2018	32	ITRC
2018 Other	2018	304	HIBP / Leak-Lookup
500px	2018	15	Gnostic
8fit	2018	20	Gnostic
Aadhaar	2018	1200	Other
Animoto	2018	25	Gnostic
Apollo.io	2018	210	Researchers
Armor Games	2018	11	Gnostic
Artsy	2018	1	Gnostic
BlankMediaGames	2018	8	Gnostic
Bookmate	2018	8	Gnostic
Cambridge Analytica	2018	87	Researchers
Chegg	2018	40	NSFW
ClassPass	2018	2	Gnostic
CoffeeMeetsBagel	2018	6	Gnostic
DataCamp	2018	1	Gnostic
DubSmash	2018	162	Gnostic
Evite	2018	10	Gnostic
Exactis	2018	340	Researchers
EyeEm	2018	22	Gnostic
Fotolog	2018	16	Gnostic
GfyCat	2018	9	Gnostic
HauteLook	2018	29	Gnostic
Houzz	2018	57	Gnostic
Jobandtalent	2018	11	Gnostic
Mariott	2018	383	Other
MyFitnessPal	2018	151	Gnostic
Netlog & Twoo	2018	57	Gnostic
Pemiblanco	2018	110	Other
PiZap	2018	61	Gnostic
Quora	2018	100	NSFW
Sephora	2018	1	NSFW
ShareThis	2018	41	Gnostic
Shein	2018	42	Gnostic
StreetEasy	2018	1	Gnostic
Stronghold Kingdoms	2018	6	Gnostic
Ticketfly	2018	28	Other
Timehop	2018	21	NSFW
Timehop	2018	21	NSFW
Wanelo	2018	23	Gnostic
WhitePages	2018	18	Gnostic
YouNow	2018	41	Gnostic

Company	Year	Records (m)	Source
2019 Cumulative	2019	64	ITRC
2019 Other	2019	80	HIBP / Leak-Lookup
Avito	2019	29	Gnostic
btcturk	2019	1	Gnostic
Canva	2019	139	Gnostic
Chinese Job Seekers	2019	202	Researchers
CodeChef	2019	8	NSFW
Coubic	2019	3	Gnostic
DailyBooth	2019	2	Gnostic
DoorDash	2019	5	NSFW
Dueling Network	2019	8	Gnostic
Epic Games (Fortnite)	2019	56	Gnostic
EstanteVirtual	2019	6	Gnostic
FemaleDaily	2019	0	NSFW
Filmow	2019	1	NSFW
First American	2019	886	Researchers
FiveStars	2019	44	NSFW
Flipboard	2019	150	NSFW
FrontLineSMS	2019	0	NSFW
Gamesalad	2019	2	Gnostic
Gatehub	2019	3	Gnostic
Hereos of Newerth	2019	4	Gnostic
iCracked	2019	2	NSFW
Indian Citizens MongoDB	2019	275	Researchers
Ixigo	2019	18	Gnostic
LifeBear	2019	4	Gnostic
LovePlanet	2019	7	Gnostic
Makaan	2019	3	Gnostic
mefedia	2019	2	Gnostic
MGM Grand International	2019	110	NSFW
MindJolt	2019	117	Gnostic
ModaOperandi	2019	1	Gnostic
MyVestigage	2019	12	Gnostic
OMGPop	2019	7	Gnostic
Overblog	2019	3	Gnostic
People Data Labs	2019	1200	Researchers
PolyCount	2019	2	NSFW
Poshmark	2019	40	NSFW
PromoFarma	2019	3	Gnostic
RedBull Sound Select	2019	1	NSFW
RoadTrippers	2019	3	Gnostic
Roll20	2019	4	Gnostic
Shein.com	2019	42	NSFW
Singlesnet	2019	16	Gnostic

Company	Year	Records (m)	Source
StockX	2019	7	NSFW
Storenvy	2019	23	Gnostic
StoryBird	2019	4	Gnostic
Tokopedia.com	2019	91	NSFW
Verifications.io	2019	780	Researchers
Voxy	2019	2	NSFW
Wirecard	2019	4	Gnostic
Yanolja	2019	1	Gnostic
Yatra	2019	5	Gnostic
YouNow	2019	40	Gnostic
Youthmanual	2019	1	Gnostic
Zynga	2019	210	Gnostic
2020 ITRC Cumulative (Q1/Q2)	2020	80	ITRC
2020 Other	2020	60	HIBP / Leak-Lookup
Accuradio.com	2020	6	Shiny Hunters / NSFW
Aptiode	2020	40	Other
AT&T - 3rd party partner	2020	40	Shiny Hunters / NSFW
Catho.com	2020	30	Shiny Hunters / NSFW
Chronicle.com	2020	4	Shiny Hunters / NSFW
DrawMyThing.com	2020	90	Shiny Hunters / NSFW
Fluke.com	2020	0	Shiny Hunters / NSFW
Foodera	2020	1	Shiny Hunters / NSFW
Leafly	2020	1	Shiny Hunters / NSFW
LivSpace	2020	20	Shiny Hunters / NSFW
Mathway	2020	25	Shiny Hunters / NSFW
Microsoft	2020	280	Other
Minted.com	2020	4	Shiny Hunters / NSFW
Omlette.com.br	2020	0	Shiny Hunters / NSFW
PlayWings.co.kr	2020	4	Shiny Hunters / NSFW
Sina Wiebo	2020	539	Other
StarTribune.com	2020	3	Shiny Hunters / NSFW
Telegram (Iran)	2020	42	Other
Tokopedia	2020	80	Shiny Hunters / NSFW
TrueCaller	2020	48	Other
Unacademy	2020	22	Shiny Hunters / NSFW
Wappalyzer	2020	16	Shiny Hunters / NSFW
Wego	2020	7	Shiny Hunters / NSFW
Wishbone	2020	40	Shiny Hunters / NSFW
Zoomcar	2020	35	Shiny Hunters / NSFW
Zoosk	2020	29	Shiny Hunters / NSFW
Zynga Poker	2020	80	Shiny Hunters / NSFW