THE DARK OVERLORD

CYBER INVESTIGATION REPORT

DATA VIPER

NIGHT LION SECURITY

TABLE OF CONTENTS

Section 1

The Dark Overlord

Executive Summary

EXECUTIVE SUMMARY

INTRODUCTION

In 2016, a hacking group known as ‘The Dark Overlord’ (TDO) began terrorizing and extorting organizations. The group quickly became known throughout the media from the large number of hacks on medical providers. Some of their first publicized hacks include Midwest Orthopedic Pain & Spine Clinic in Farmington, MO, Midwest Imaging Center, LLC, and Van Ness Orthopedic and Sports Medicine.

In 2017, the group gained additional headlines for hacking Netflix and threatening to release advanced copies of ‘Orange is the New Black’ if their ransom demands were not met.

Later that year TDO moved from traditional “hacking” to more terror-based attacks, when the group began sending life-threatening messages to the parents of students in the Columbia Falls, Montana school districts, causing the closure of more than 30 schools, and forcing more than 15,000 students to stay home for an entire week.

This report was developed by Vinny Troia, founder of Night Lion Security and Data Viper, and only contains a subset of the discovered evidence.

For additional details and a more-personal account of the TDO investigation, please consider picking up a copy of my book, "Hunting Cyber Criminals", available on December 1, 2019.

Section 2

The Dark Overlord

Introduction

2.1

THE DARK OVERLORD

BEGINNINGS

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.

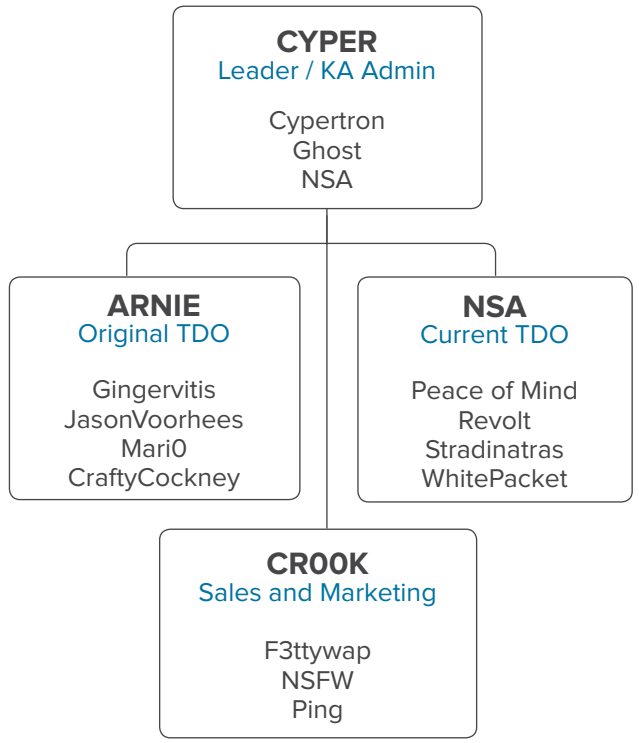
GROUP STRUCTURE

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 is led by Cyper, the admin of the KickAss forum. The group was formed circa 2015. It is believed that the members met on Hell, an old dark web hacking forum.

Cr00k appeared to be the person in charge of marketing and selling the stolen data, while NSA assisted in the hacking and extorting of additional victims.

In 2017, TDO publicly announced a change in leadership over Twitter, during which time it is believed that command of the group was transferred from Arnie (TDO1) to NSA (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
VICTIMOLOGY

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

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

2.3

FORUMS AND MARKETS INDEX

BLACKBOX (BB)

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

EXPLOIT.IN (EI)

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).

SIPH0N

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.

2.4

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 derrived 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/

2.5

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 enfrorcement agencies wanting adversarial threat intelligence.

For more information, visit www.dataviper.io

Section 3

The Dark Overlord

History & Operating Procedures

3.1

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 initiall used by the group was backdoor access to the HL7 Healthcare software. In an interview with DataBreches.net [5], TDO made the following statement,

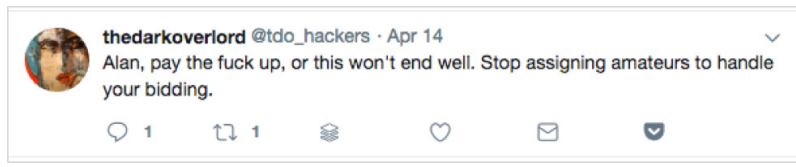
> *"I used their code to find exploits in all their clients.... Also, since I was in their system, I signed a backdoor into their client – because I had access to their certificate signing. It got pushed out in an update a few weeks ago."*

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.databreaches.net/hl7-vendor-hack-compromised-clients-ehr-records-the-dark-overlord/

3.2

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 (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, most likely 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 his 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.

3.3
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).

3.4

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/qkjzpx/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

3.5

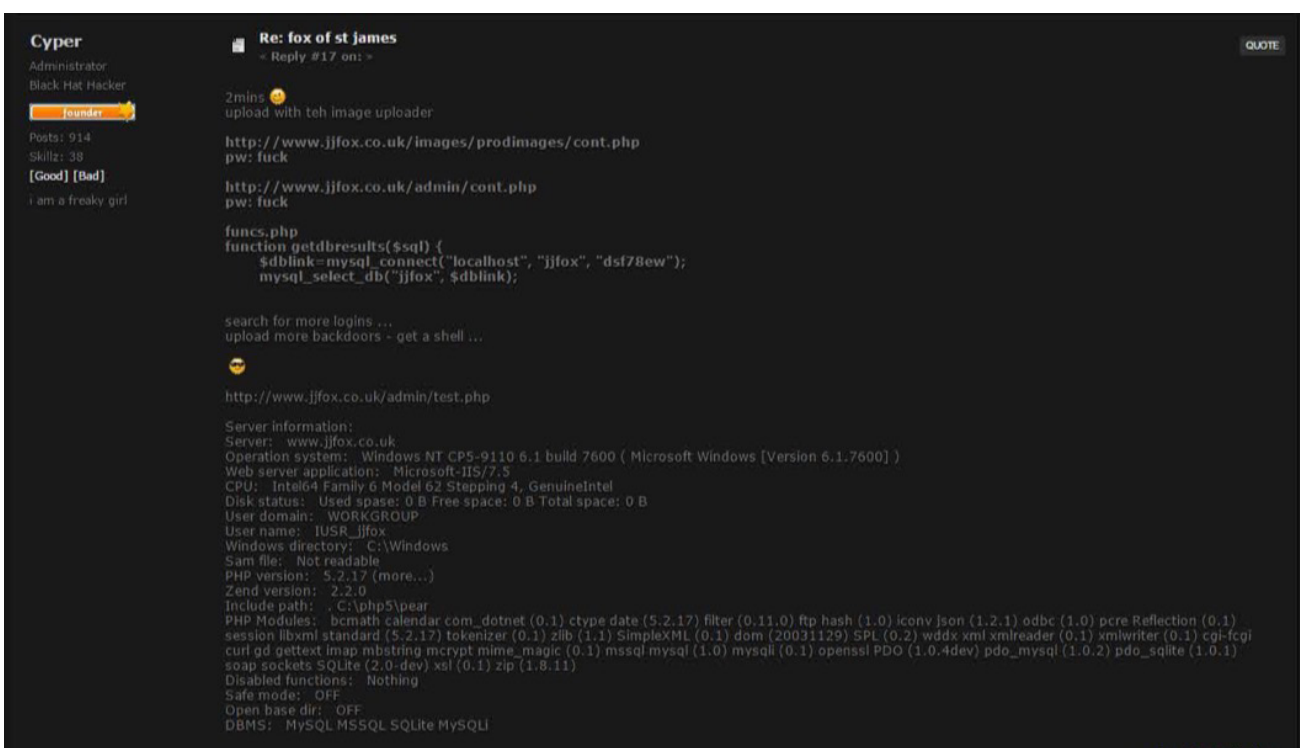
GROUP FORMATION

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, Hexxx, Gingervitis, Zer0ing (four of which are believed to have played an active role in the group).



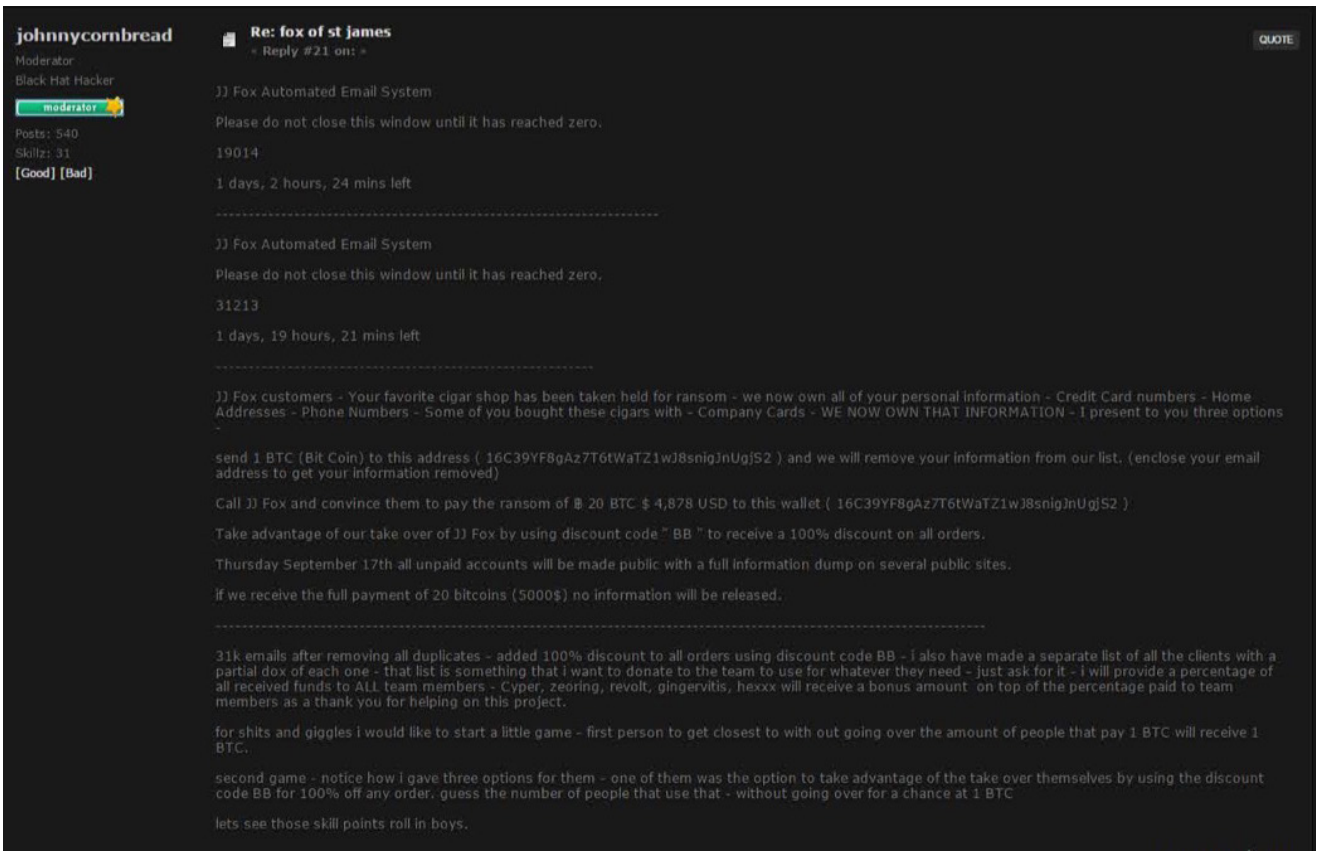
PRE-TDO:
A GROUP RANSOM PROJECT

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.*



johnnycornbread
Moderator
Black Hat Hacker
moderator
Posts: 540
Skillz: 31
[Good] [Bad]

Re: fox of st james
« Reply #21 on: »

QUOTE

JJ Fox Automated Email System

Please do not close this window until it has reached zero.

19014

1 days, 2 hours, 24 mins left

JJ Fox Automated Email System

Please do not close this window until it has reached zero.

31213

1 days, 19 hours, 21 mins left

JJ Fox customers - Your favorite cigar shop has been taken held for ransom - we now own all of your personal information - Credit Card numbers - Home Addresses - Phone Numbers - Some of you bought these cigars with - Company Cards - WE NOW OWN THAT INFORMATION - I present to you three options -

send 1 BTC (Bit Coin) to this address (16C39YF8gAz7T6tWaTZ1wJ8snigJnUgjS2) and we will remove your information from our list. (enclose your email address to get your information removed)

Call JJ Fox and convince them to pay the ransom of ฿ 20 BTC $ 4,878 USD to this wallet (16C39YF8gAz7T6tWaTZ1wJ8snigJnUgjS2)

Take advantage of our take over of JJ Fox by using discount code " BB " to receive a 100% discount on all orders.

Thursday September 17th all unpaid accounts will be made public with a full information dump on several public sites.

If we receive the full payment of 20 bitcoins (5000$) no information will be released.

31k emails after removing all duplicates - added 100% discount to all orders using discount code BB - i also have made a separate list of all the clients with a partial dox of each one - that list is something that i want to donate to the team to use for whatever they need - just ask for it - 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.

for shits and giggles i would like to start a little game - first person to get closest to with out going over the amount of people that pay 1 BTC will receive 1 BTC.

second game - notice how i gave three options for them - one of them was the option to take advantage of the take over themselves by using the discount code BB for 100% off any order. guess the number of people that use that - without going over for a chance at 1 BTC

lets see those skill points roll in boys.

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

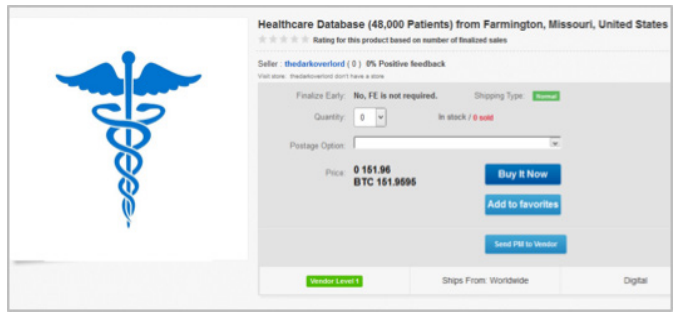
3.6

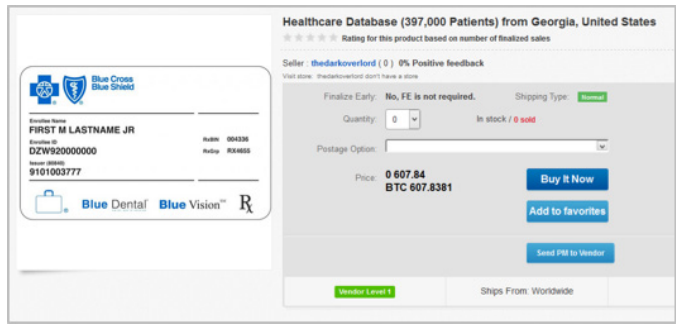
TDO'S FIRST APPEARANCES

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.

3.7

INITIAL MEMBERS

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.

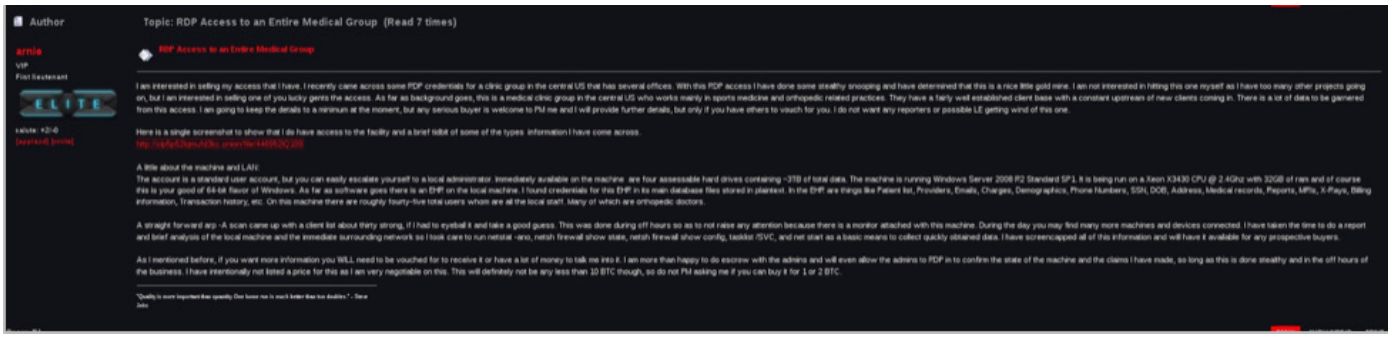
ARNIE

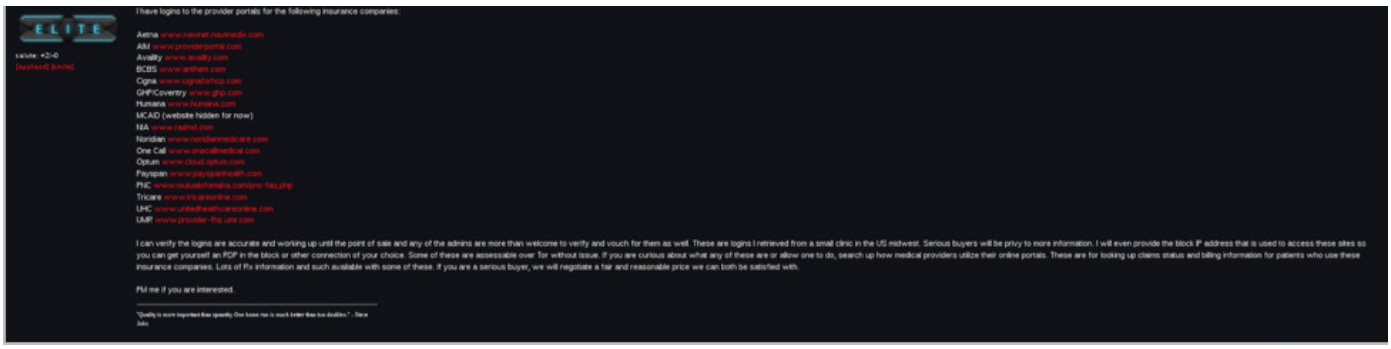
The 'Arnie' moniker made his first appearance on Hell Reloaded. Arnie was only active for a few months using this name but quickly became known as the group's leader throughout the security community and underground forums.

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

> *Admittingly, 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.



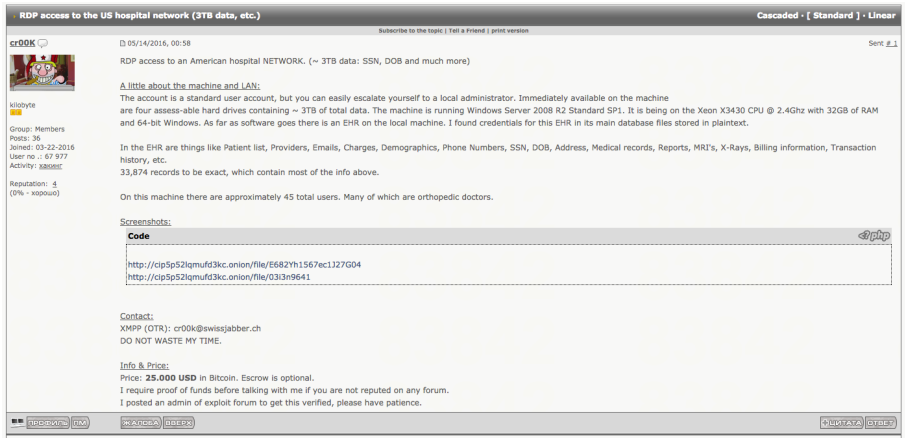


CR00K

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, usin the same contact information.

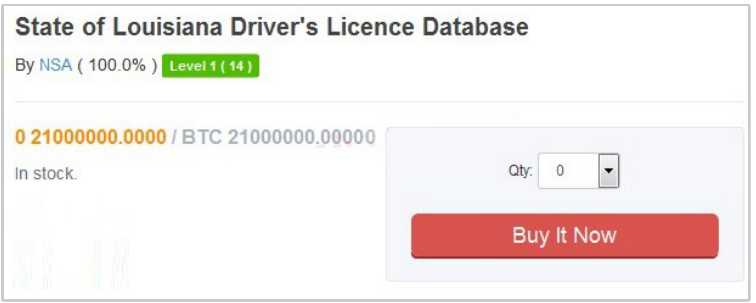
Identical posts were made on Siph0n forum under user F3ttywap, contact address w4p@exploit.im.



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 is 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).

THEDARKOVERLORD
@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: ahhahahahhahahahah

3.8

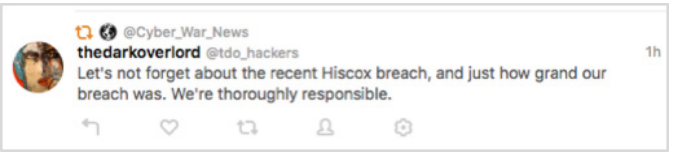
DE-EVOLUTION OF THE GROUP

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.

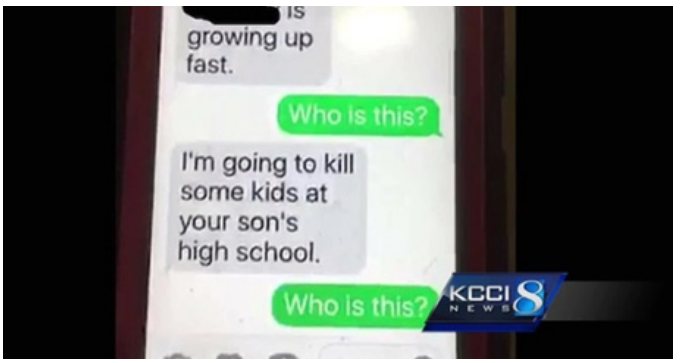
TDO would then contact those medical providers claiming they had been breached, offering non-existent or recycled patient information as evidence of their access.



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://1qb1ow3qfudf14kwjzalxq61.wpengine.netdna-cdn.com/wp-content/uploads/2017/09/Letter-with-redaction.pdf

3.9

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.

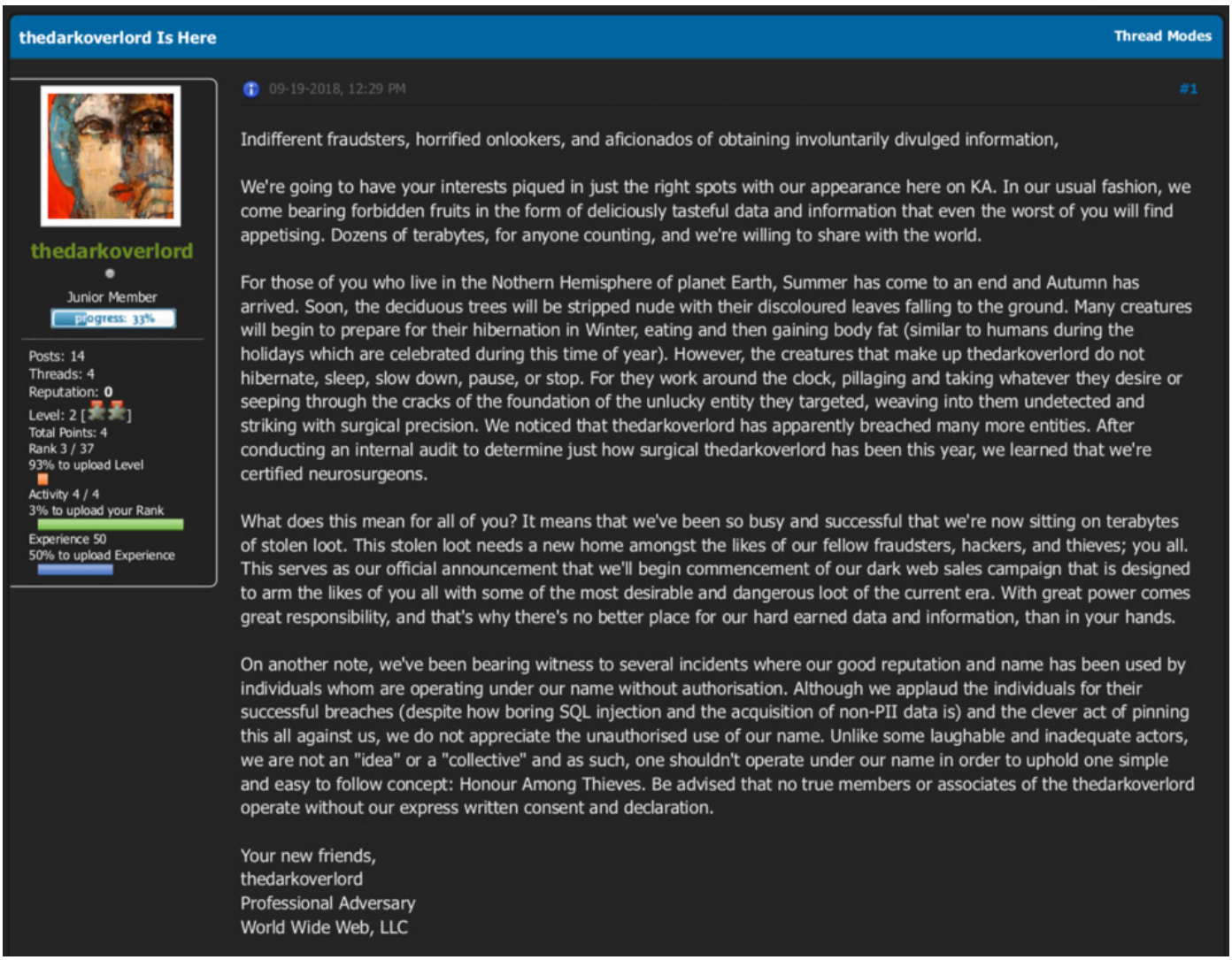
VT:	So how are things in overlord land?
4vmc3txofm:	You mentioned NSA's name.
VT:	i dont' believe i did?
4vmc3txofm:	"You have the marketing pull and the ability to get media's attention. that's what i'm after. My backup would be to go to NSA but i dont think he can create the same buzz you can."
VT:	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/

3.10

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.

3.11

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@torbox3uiot6wchz.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.

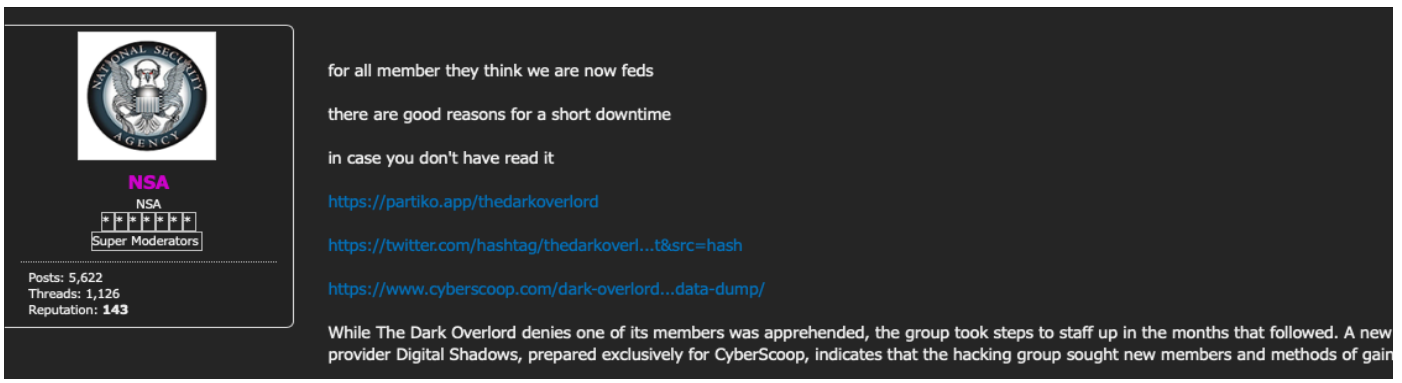
This is the exact tactic and seizure notice used when Cyper shut down his BlackBox forum in 2017.

3.12

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, a friend 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: lmo, 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 certintly did not mean for KickAss to be shut down. Sorry!

SECTION 4

The Dark Overlord

Threat 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 respoective sections.

	Actor	Member	Role	Aliases (Partial)	Real Name	Location
4.2	Cr00k	N	Sales / Marketing	Ping Photon NSFW	Dennis Karvouniaris	Calgary, Canada
4.3	NSA	Y	Hacker / Lead (TDO2)	Revolt Obfuscation Peace of Mind Stradinatras WhitePacket	Christopher Meunier	Calgary, Canada
4.4	Arnie	Y	Hacker / Initial Lead (TDO1)	CraftyCockney Gingervitis JasonVoorhees Mari0 Mas	Nathan Wyatt	United Kingdom
4.5	Cyper	Y	Capo	Cypertron Cypertr0n Ghost NSA X3n0n	Unknown	Austria

4.2

Name: Dennis Karvouniaris (DK)

CR00K

Age: 18 Location: Calgary, Canada

ALIASES

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

AFFILIATIONS

Hell (Founder)
Hell Reloaded (admin)
TheRealDeal
Gnostic Players

JABBER IDS

btc@richim.org
c86x@blackjabber.cc
chms@jabber.se
columbine@xmpp.jp
cr00k@swissjabber.ch
frosty@digitalgangster.com
nsfw@jabber.se
ping@rows.io
russian@xmpp.is
sepa@swissjabber.ch

SOCIAL MEDIA

instagram.com/dio_the_plug

CONFIRMED HACKS (PARTIAL)

Adult Friend Finder
Army Force Online
Bell.ca
BotofLegends
CardingMafia
CodeChef
Datalot
Door Dash
DotaHut
FIlmNow
FiveStars
Flipboard
GSMA Intelligence
iMesh
Linux Mint
Livspace
Moda
MGM Grand
Poshmark
Redbul
Sephora
StockX
TeamSkeet
Timehop
Tokopedia
Voxy

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 is 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 realted 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,Email,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 Peace of Mind and Prometheus

B. Additional Attribution Between Prometheus to TDO

C. Connecting Prometheus to NSFW and Photon

D. Connecting NSFW to Ping and Cr00k

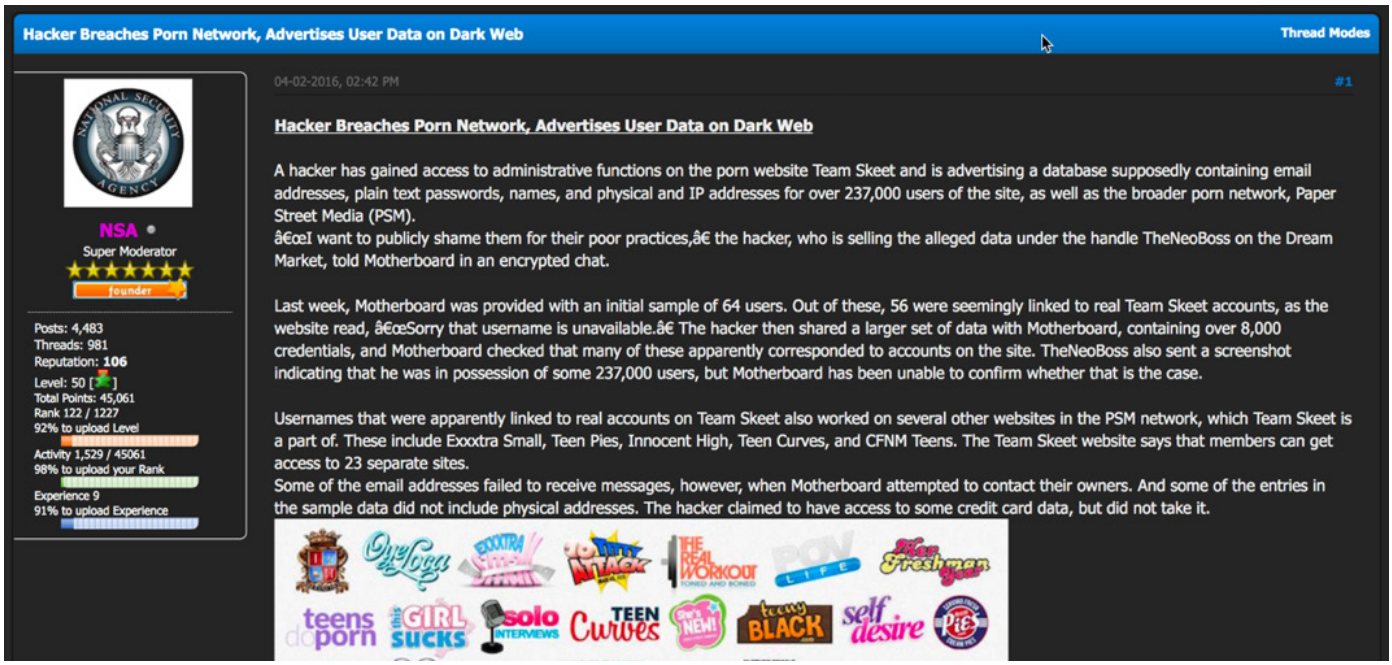
E. Who is the Real Ping?

4.2.2.A

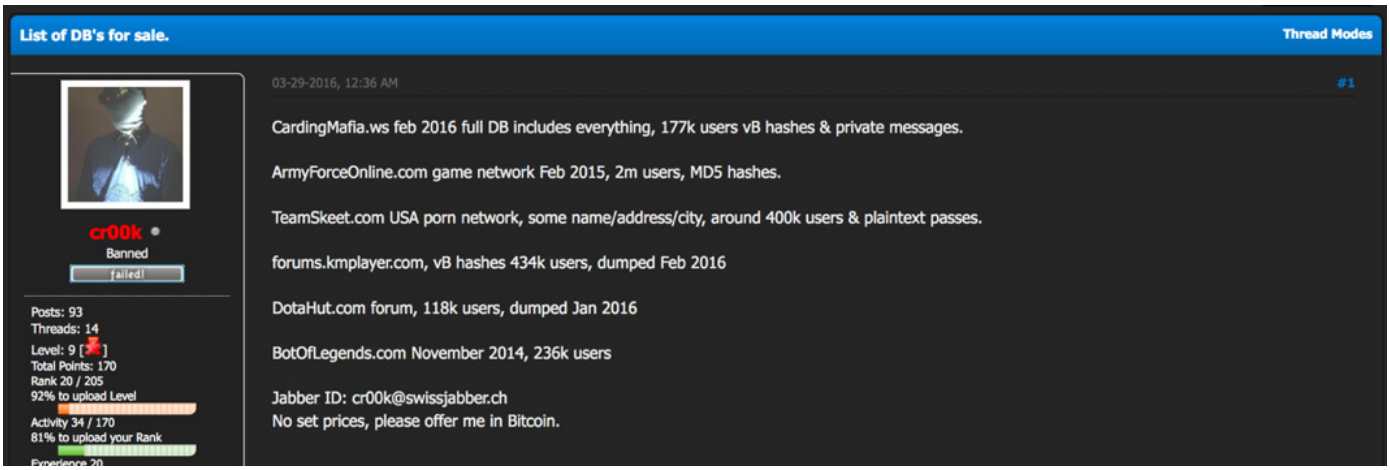
LINKING CR00K TO PEACE OF MIND AND PROMETHEUS

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

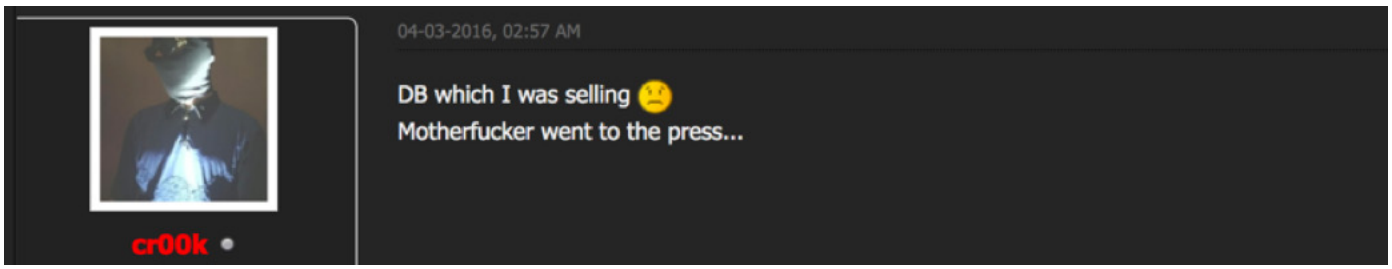
1. Article posted on KA regarding a hacker's breach into a number of porn sites, such as Team Skeet.



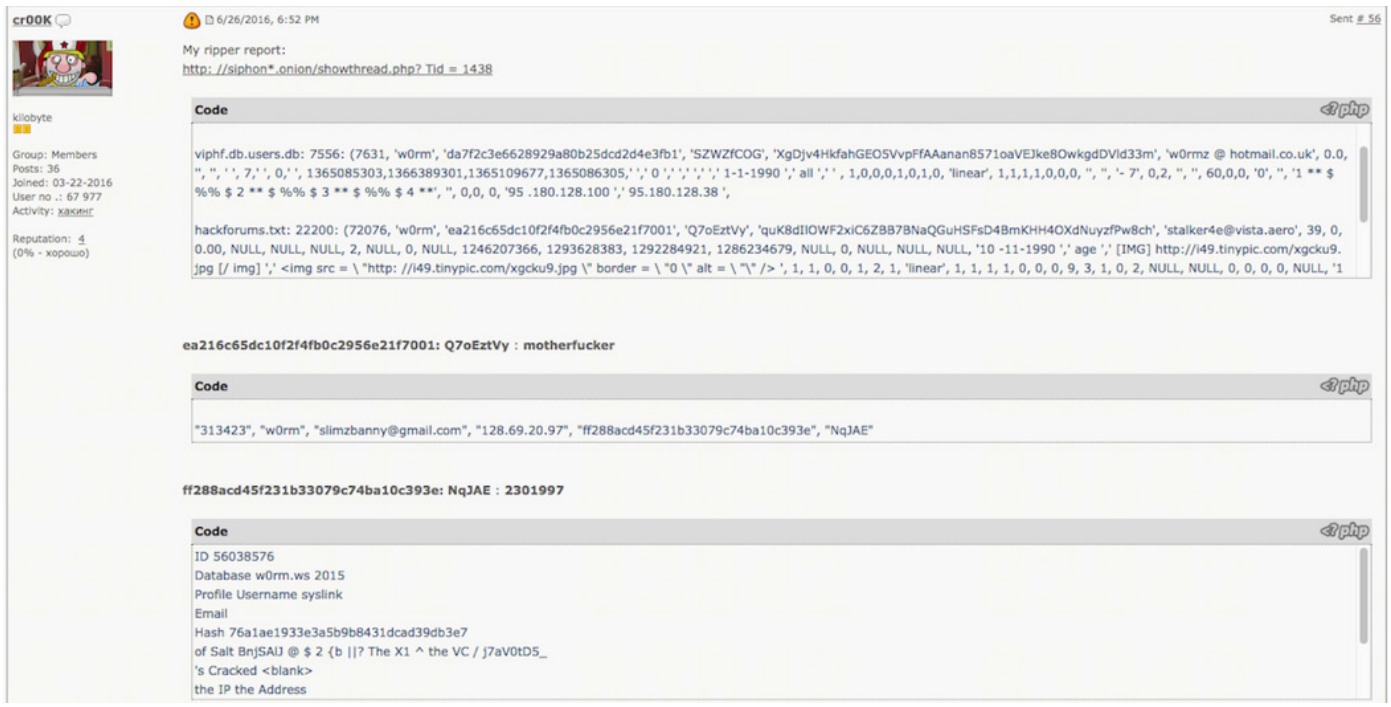
2. User cr00k selling Team Skeet (and other) data on KA.



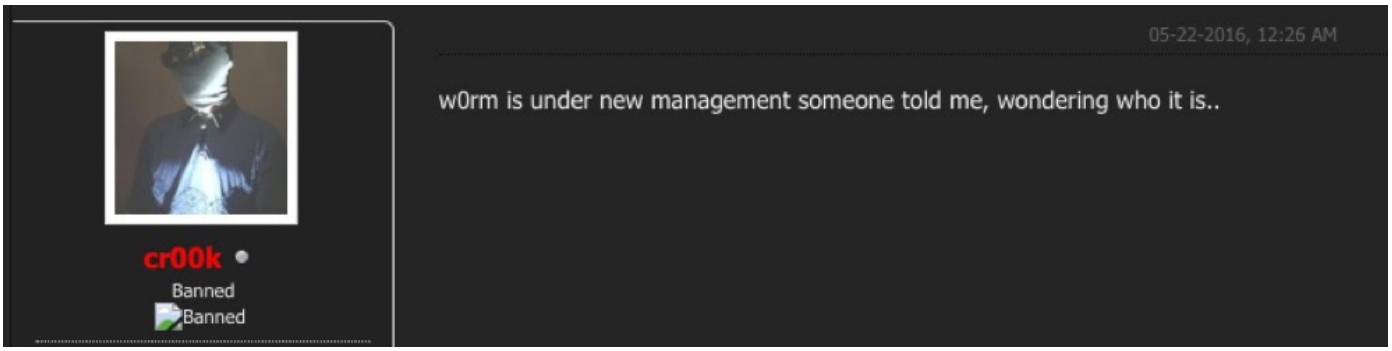
3. User “NeoBoss” (aka Worm) contacts Joe Cox of Motherboard and takes credit for the hack.[14] W0rm publicly released the database that cr00k was selling, effectively making it worthless.



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 transfered 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.

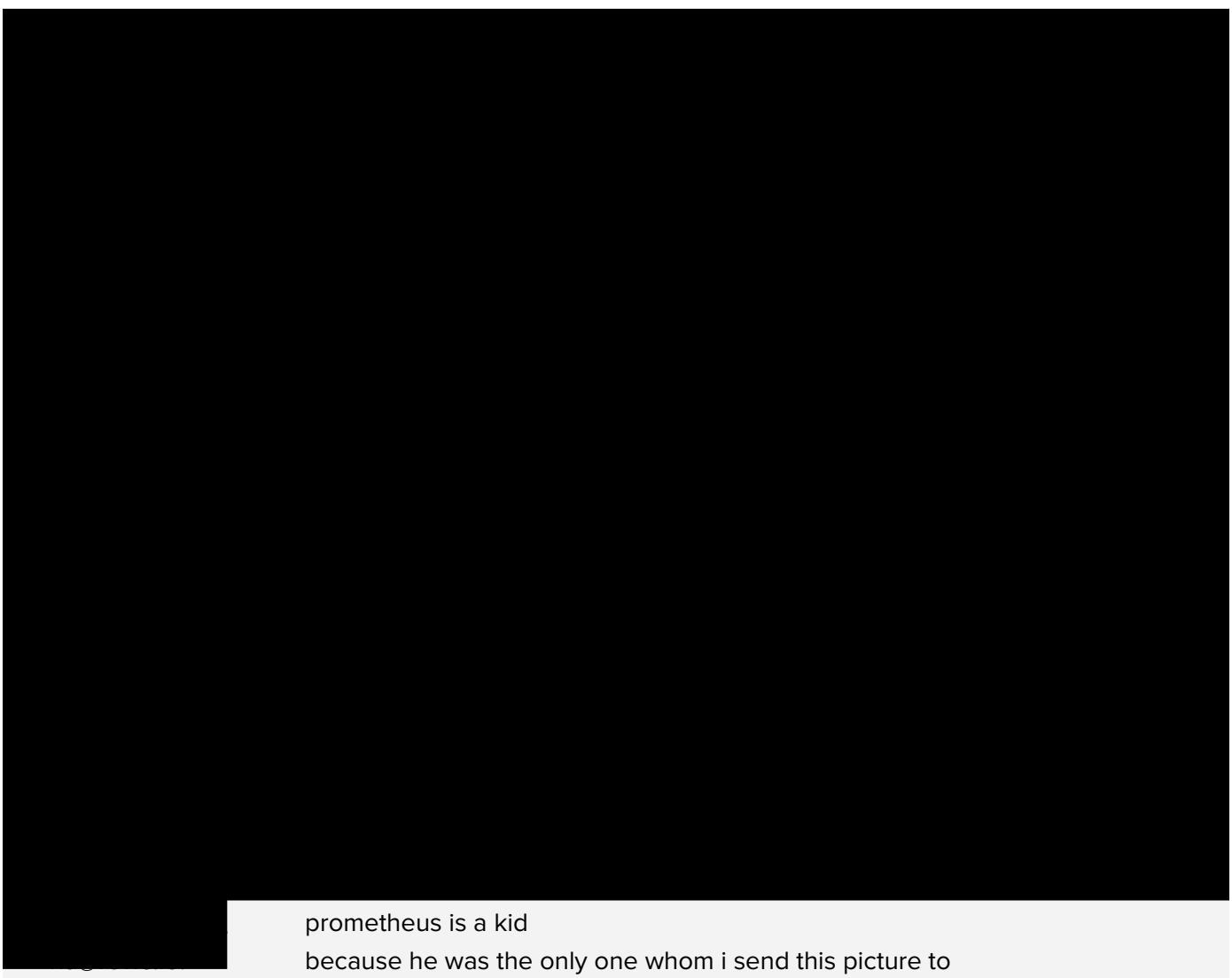
Based on this evidence, ke7hb and Cr00k are associated with Peace of Mind and Prometheus. Subsequent sections of this report will determine which users are connected.

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] angirly 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

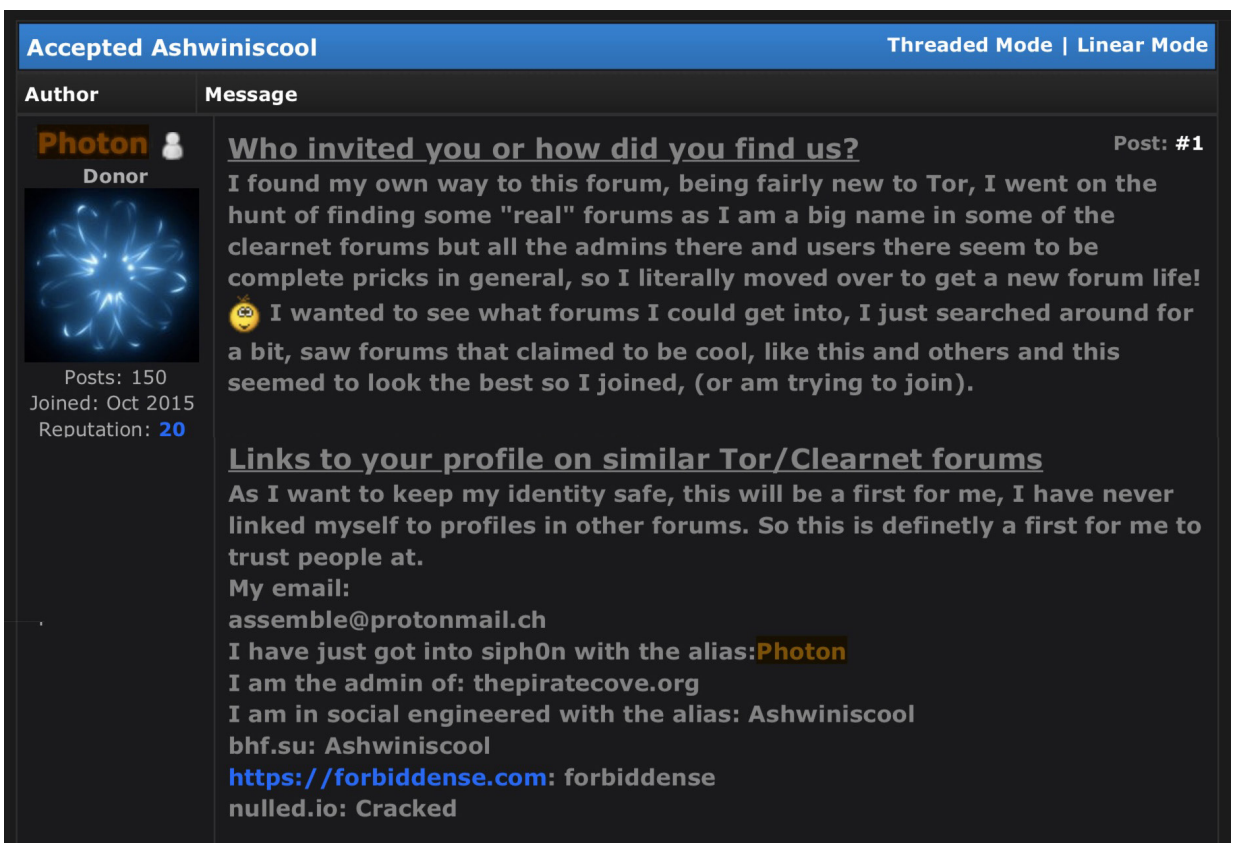
CONNECTING PROMETHEUS TO NSFW AND PHOTON

PHOTON'S INTRODUCTION TO 0DAY FORUM

User Photon (0day 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 avaialble 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 0day forum, using the email address assemble@protonmail.ch.



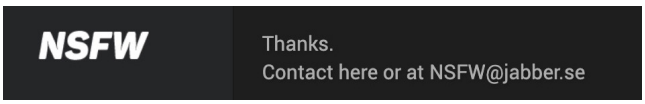
Note: *In the same way Cr00k also leads to a carder in Canada, we believe the name Ashwin, aka Ashwiniscool, is a trap to lead researchers directly down the wrong path. Cr00k is highly skilled at associating himself with names that can easily be traced to other people.*

ATTRIBUTION BETWEEN PHOTON AND NSFW

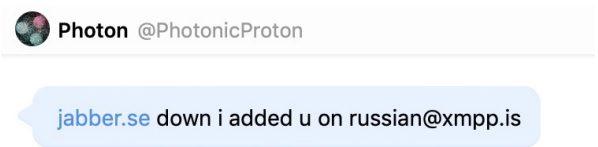
1. In the following private conversation, user Photon is revealed as also being NSFW, Ryder and Prometheus.

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 over RaidForums.com. The following screenshot shows a post by NSFW on offering his jabber account, nsfw@jabber.se.



3. At times, conversations with NSFW would move fluidly between his Twitter account, PhotonicProton, and his other jabber accounts:
   russian@xmpp.is
   btc@richim.org



Each of the three jabber accounts logged-in and off at exactly the same time, and the conversation was easily interchangeable between any of the accounts.

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, Photon, and NSFW.

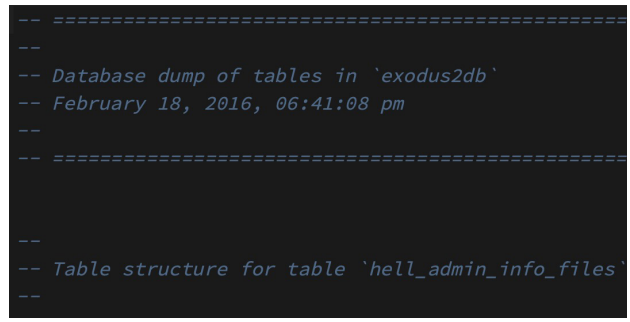
XX:	why did he send you his pictures
Russian:	pictures?
Russian:	that was ages ago
Russian:	when i decided i was done with him
Russian:	and he was useless
Russian:	i social engineered him
Russian:	and sent fake pictures of myself
Russian:	and he trusted me and sent me his
Russian:	and i also found out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

4.2.2.D

CONNECTING NSFW TO PING AND CR00K

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 0day introduction post.

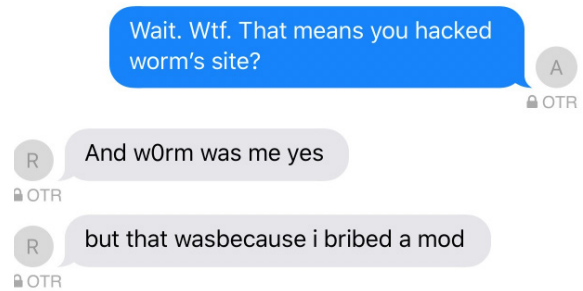
```
INSERT INTO smf6_members VALUES('1', 'peace', 'peace@rows.io', '', '0', '0001
INSERT INTO smf6_members VALUES('2', 'Lava', 'assemble@protonmail.ch', '', '0
INSERT INTO smf6_members VALUES('3', 'TheRealDeal', 'trdtrd@mailinator.com',
```

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 NSFW 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 NSFW and Ping are the same person.

NSFW ADMITS TO HACKING W0RM.WS

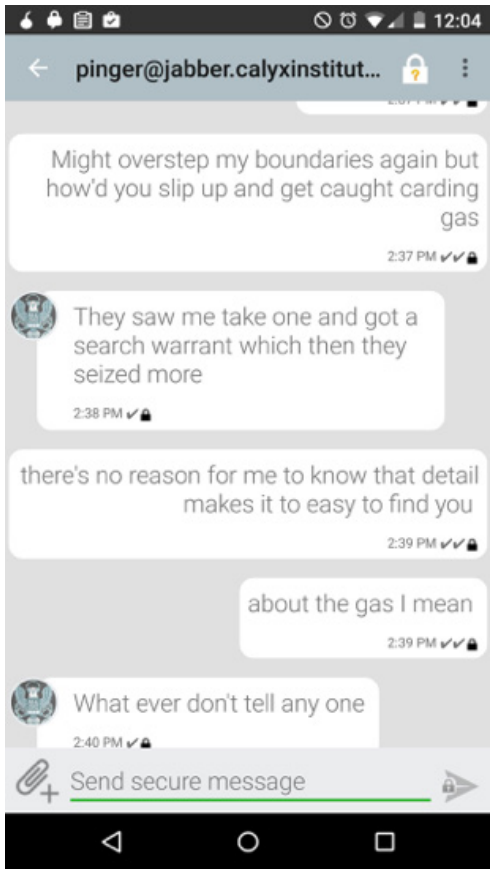
During a private chat, NSFW admits to hacking the w0rm.ws site by bribing a moderator. Based on the previous analysis of the leaked w0rm database, the "mod" is ke7hb.



4.2.2.E

WHO IS THE REAL PING?

A STORY OF DECEPTION AND MEDIA MANIPULTION



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

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, a core (but former) 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 'Ping', as the owner of Hell forum and Photon.

His most recent alias, NSFW, is responsible for a number of high profile

KNOWN ALIASES

- AmiEdgyEnough
- c86x
- Columbine
- Cr00k
- Jinn
- Malum
- Nakk3r
- NSFW
- Overflow
- Photon
- Ping
- Rejoice
- ROR[RG]
- Ryder

ATTRIBUTED HACKS

The following hacks can be attributed to one of DK's aliases

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

4.3

Name: Christopher Meunier (CM)

NSA

Age: 19 Location: Calgary, Canada Phone: 587 999 5631

ALIASES

Diablo
F3ttywap
Frosty
L3tm3
Mastercorp
NSA
Obfuscation
Peace
Peace of Mind
Revolt
ROR[RG]
Soylent
Stradinatras
The_Dick_Head
Trickster
Vladimir
WhitePacket
ZLO

AFFILIATIONS

TheRealDeal
KickAss
CanadaHQ

JABBER IDS

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 WP took over as leader of TheDarkOverlord in 2017.

Evidence suggests CM, also known as NSA, is the group's primary hacker. WP is believed to be responsible for the development of several paid botnets, hacking the Louisiana DMV, iMesh, Mate1, and may be involved in the use and distribution of the Mirai Botnet. Evidence also suggests that WP is the owner and operator of CanadaHQ.at, a darkweb marketplace focused on Canadian-based crime.

It is believed that CM works (or has worked) for Alt8 Communications, a cybersecurity consulting firm owned by his father, William Meunier.

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

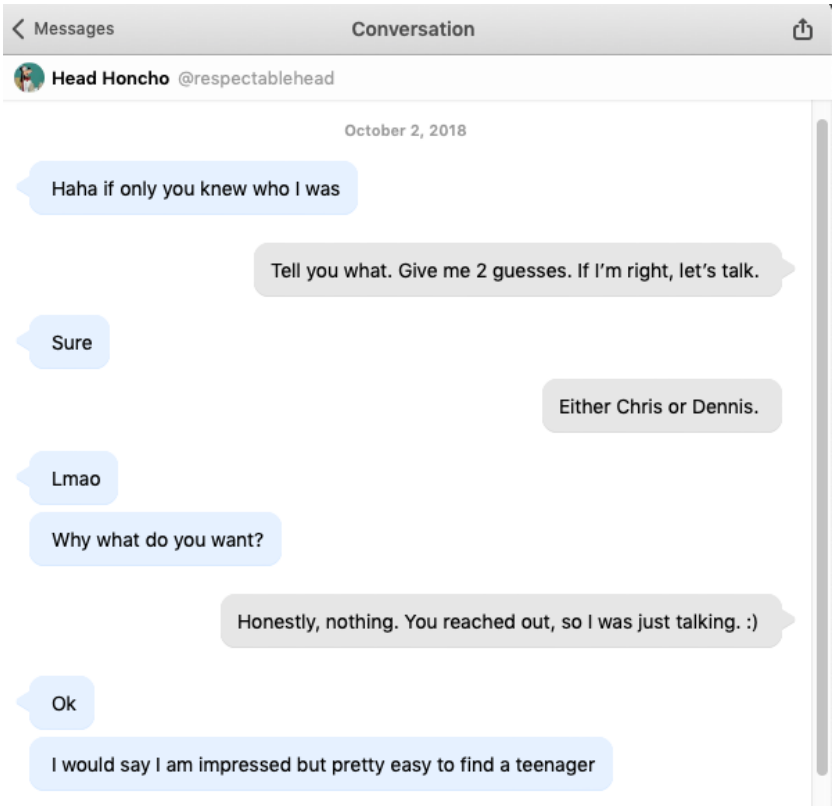
RELATIONSHIP WITH DK

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.

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 ORGANIZTIONS

ATTRIBUTION SECTIONS

A. Revolt, WhitePacket, ZLO, and Vladimir

B. Peace of Mind and the W0rm Hack

C. Peace and TheRealDeal Market

D. NSA, Revolt, and Diablo

E. Linking CM to Stradinatras and Obfuscation

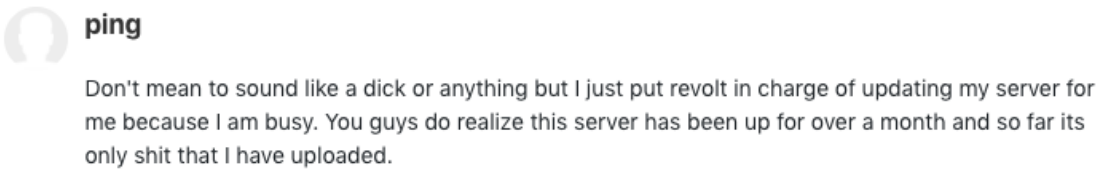
4.3.3.A

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.



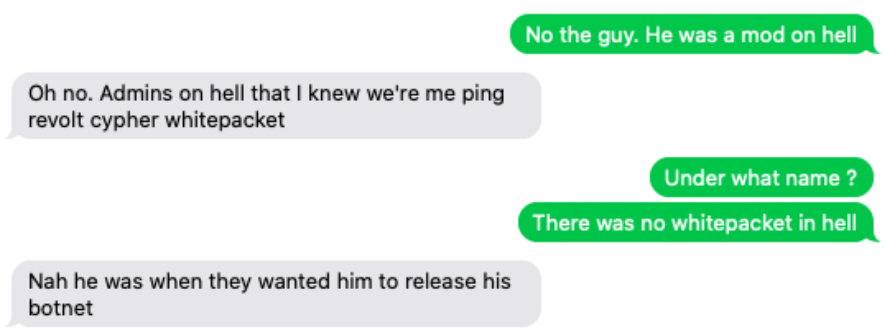
ZLO PARTNERSHIP

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.



CM ADMITS TO BEING ZLO AND VLADIMIR

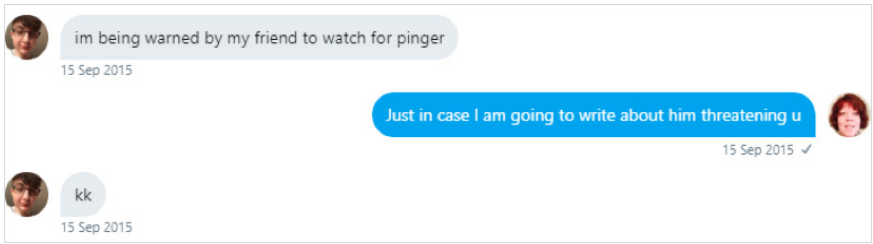
In 2016, CM began speaking to tech reporter Bev Robb over Twitter regarding his association with Hell forum, and his volitile relationship with Ping.

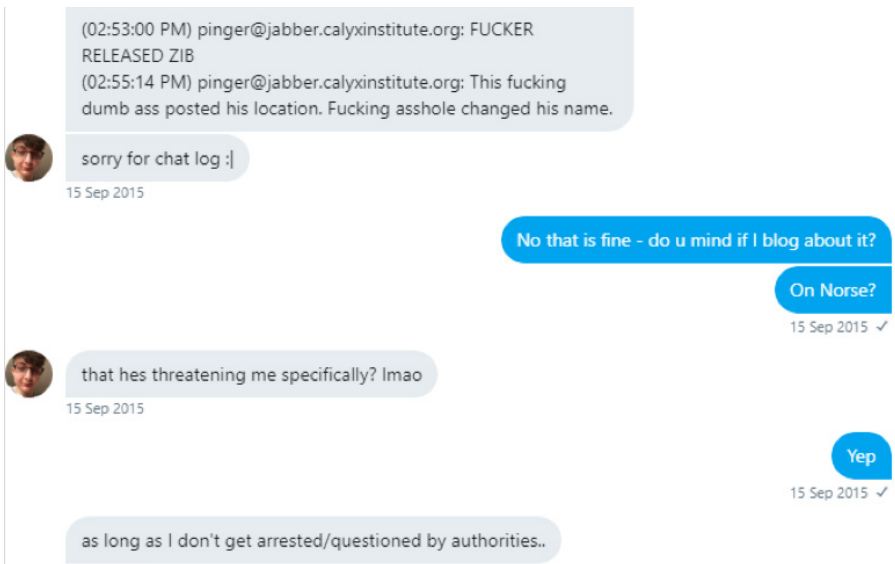
A number of private conversations occurred between WP and tech reporter Bev Rob. The following screenshot shows WP taking credit for writing the ZiB botnet and admits to being users “ZLo” and “Vladimir” on Hell forum.

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 W0RM 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 W0RM HACK & KE7HB

Logs from leaked w0rm.ws forum dump show that user ke7hb ultimately transfered 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

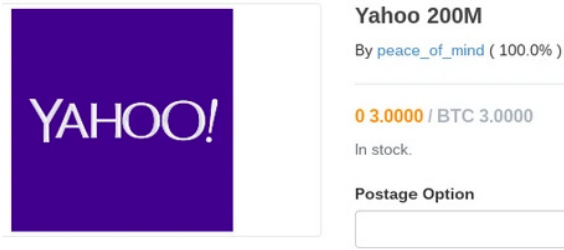
The chain of events surrounding the w0rm hack, and analysis of the forum's leaked data, indicate that that users data2z@swissjabber.org and cr00k@swissjabber.ch are two different people, both associated with The Dark Overlord.

4.3.3.C

PEACE AND THEREALDEAL MARKET

WHO IS PEACE OF MIND?

Peace of Mind initially gained noteriety through the advertising and sale of several high profile data breaches including Yahoo, LinkedIN, MySpace, Tumbler, 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

> *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 anb 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 evidence and details surrounding this connection are available in Vinny Troia's upcoming book, "Hunting Cyber Criminals", available December 2019 on Wiley.

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 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.

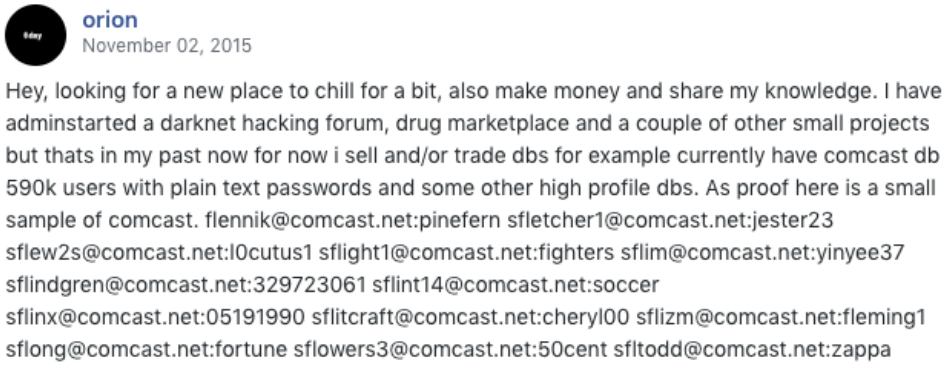
ORION

The following is an excerpt from a private conversation between a security researcher and Ze0ring (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 0DAY FORUM

During his application post on the 0day 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 0day, 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
0day
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 execpt 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/Clearnet 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, 0-day and Siph0n 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

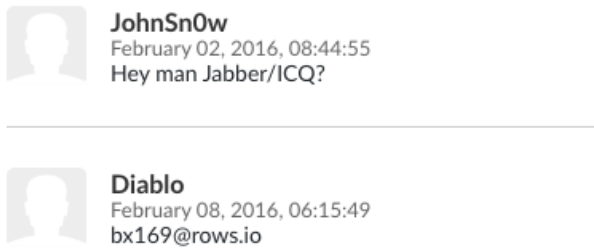
During a private conversation over jabber chat, actor NSFW (DK) links alias Revolt to himself and NSA (from TDO)

> 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.

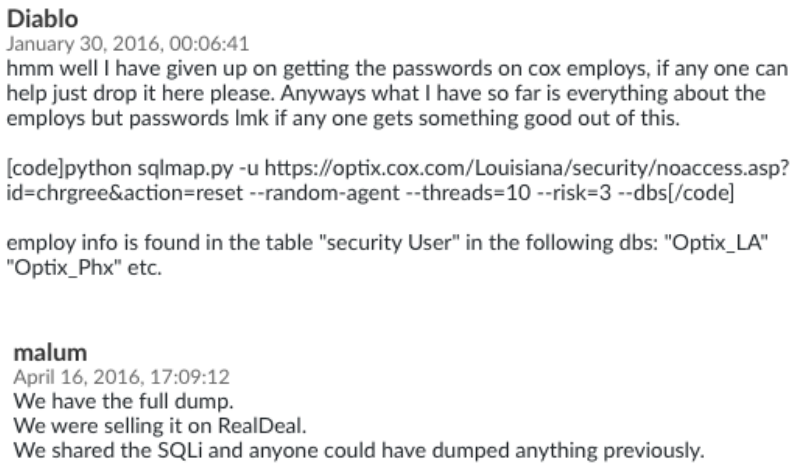
Diablo uses the jabber address bx169@rows.io, previously connected to Peace of Mind.



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.



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.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, WP 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 0day application post.*

4.3.4

SUMMARY

Summary of user NSA and and his association to WP

Christopher Meunier (WP), 19, of Calgary Canada is believed to be the individual behind the personas of several significant threat actors, including Peace of Mind, 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 NSA (nsa@rows.io) is believed to be responsible for hacking the Louisiana DMV, Mate1, and imesh, 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.

KNOWN ALIASES

- Diablo
- Frosty
- L3tm3
- Mastercorp
- NSA
- Obfuscation
- Peace
- Peace of Mind
- Revolt
- ROR[RG]
- Soylent
- Stradinatras
- Trickster
- Vladimir
- Vladimir696
- WhitePacket
- ZLO

4.4

Name: Nathan Fyffe Wyatt (NW)

ARNIE

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

ALIASES

Arnie
CraftyCockney
DarkMoneyMan
Gingervitis
JasonVoorhees
l00t5
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 the Dark Overlord, and was also the group's original lead figure under the alias Arnie.

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 is currently facing extradition to the U.S. on several charges related to crimes associated with The Dark Overlord group.

NW was believed to be a member of the Hell forum and BlackBox as Gingervitis, and on KickAss as JasonVoorhees.

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 allegidly opened bank accounts in both his and his girlfriend's name which were used to withdraw funds from TDO extortions. [18]

This report also shows other instances where CM and DK attempt to pin their crimes on others.

PRIVATE FACEBOOK CONVERSATION LOGS

Despite Wyatt's obvious need to deny any involvment 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.

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

Additional conversations are included on the next page.

In those conversations, 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 grammer.

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

17 https://www.databreaches.net/tag/thedarkoverlord-the-dark-overlord/

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

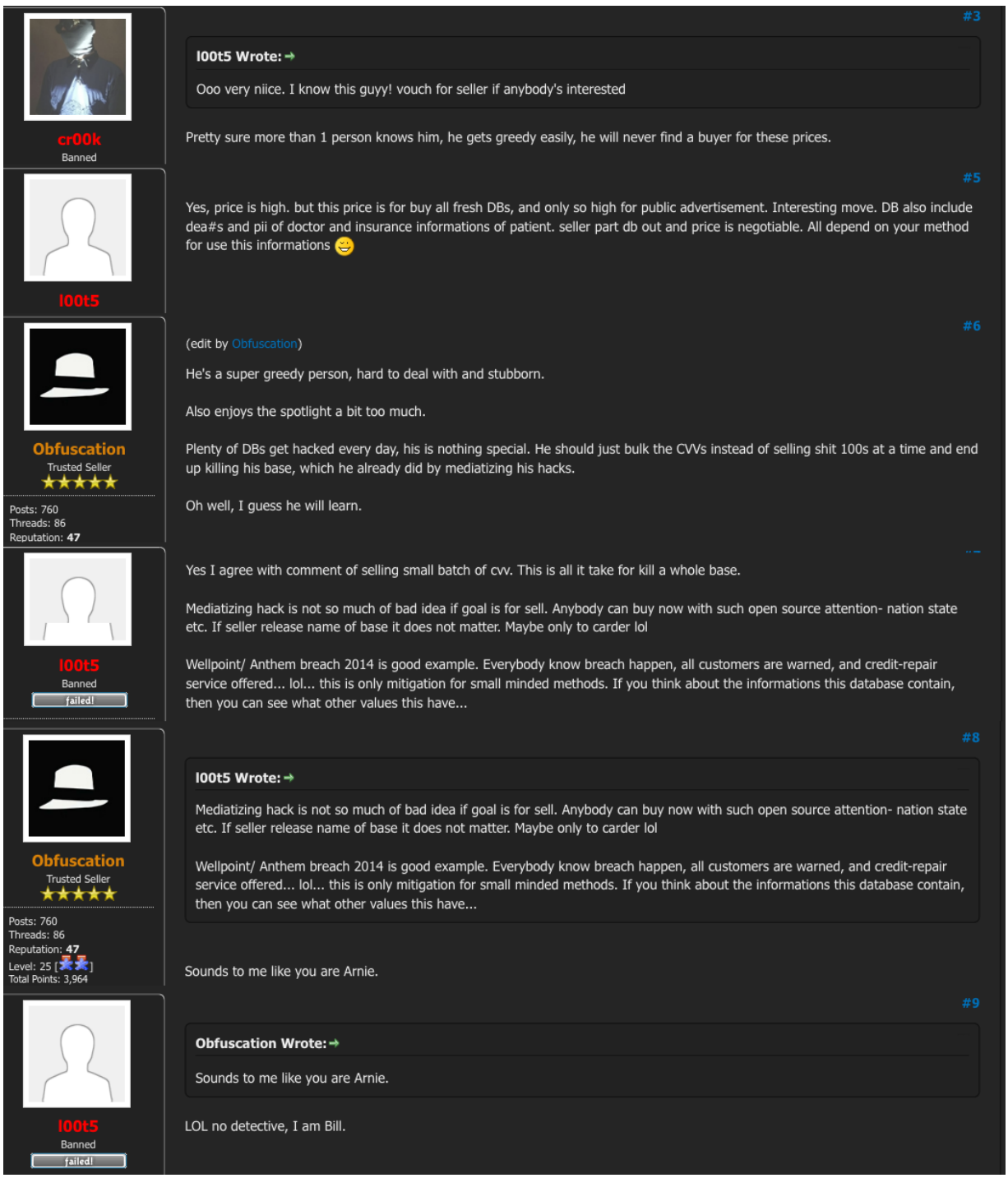
Reputation..professionalism ... the tdo I know... **would spaz out make threats be aggressive**

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 l00t5 vouches for the sale of TDO's medical data. Obfuscation (WP) outs l00t5 as being Arnie. L00t5 instead refers to himself as "Bill".



cr00k
Banned

#3

l00t5 Wrote:

Ooo very niice. I know this guyy! 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.

l00t5

#5

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

Obfuscation
Trusted Seller
Posts: 760
Threads: 86
Reputation: **47**

#6

(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.

l00t5
Banned
failed!

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...

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

#8

l00t5 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.

l00t5
Banned
failed!

#9

Obfuscation Wrote:

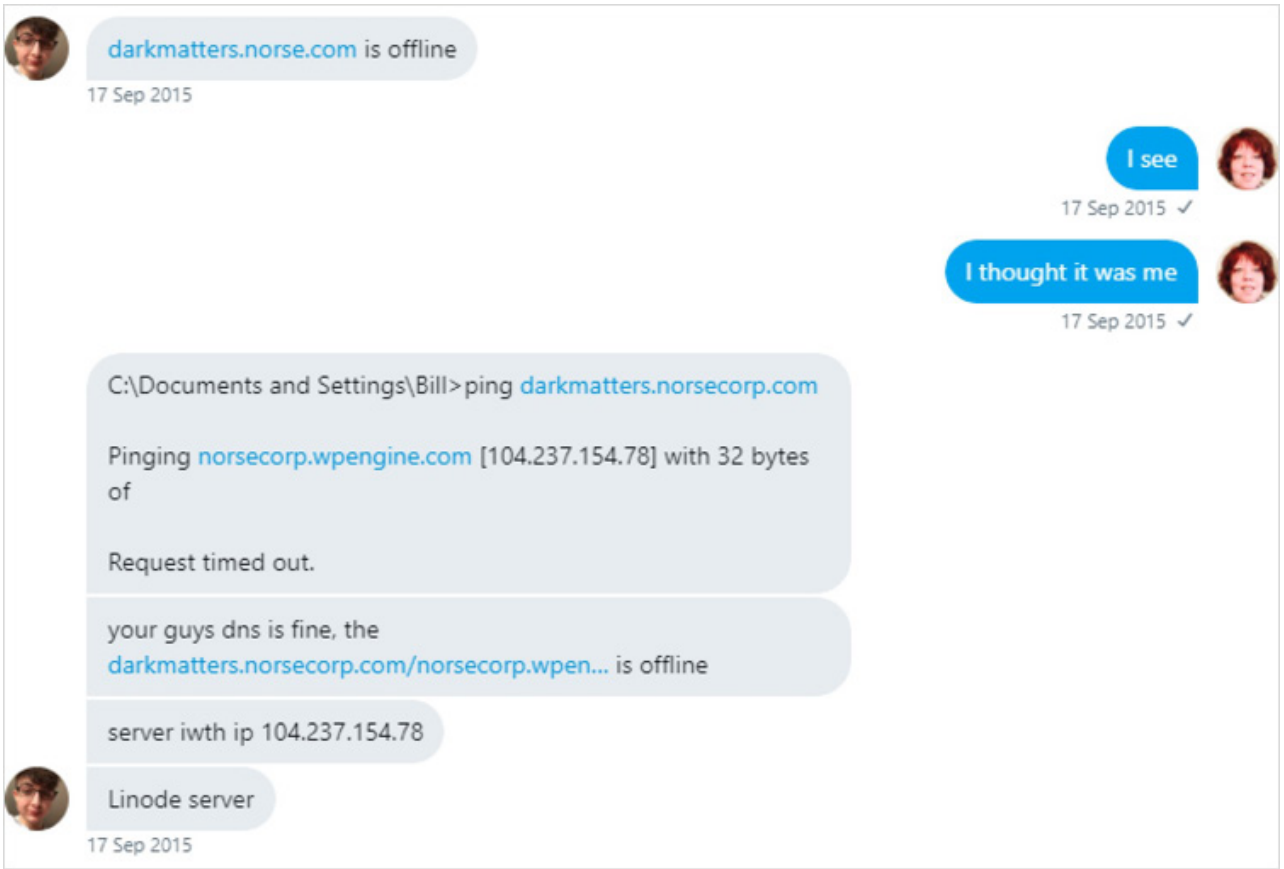
Sounds to me like you are Arnie.

LOL no detective, I am Bill.

4.4.4

WHO IS BILL?

Bill, or William Meunier, is WP's father, and owner of Alt8 Communications, Inc.
In private conversations with Bev Robb over Twitter, WP sends Robb a paste of his windows terminal. The username of his computer is Bill.



ANALYSIS AND THEORY

In other conversations, WP refers to using his father's computer when logging onto XMPP. It is our theory that user Obfuscation (WP) knew l00t5 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 WP (TDO 2).

Arnie (l00t5), having a history with WP, could have easily known Bill to be WP's father's name. It is possible he also saw similar screenshots and thought WP's name was Bill.

When WP outed l00t5 on KickAss as being Arnie, l00t5 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,” faces 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 transfered 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*

4.5

Name: Unknown

CYPER

Probable Age: 40s Location: Austria

ALIASES

NSA
Ghost
Cyper
Cypertron
C3nt3rx
X3non
L00k

JABBER IDS

nsa@jabber.calyxinstitute.org
ka_apps@jabber.calyxinstitute.org

SOCIAL MEDIA

http://twitter.com/cypertr0n

AFFILIATION

Hackweiser
SleeperS crew
KickAss Forum
BlackBox

BACKGROUND

Cyper (no H) boasts himself to be a hardcore C++ programmer with 20+ years of experience in the field. His experience in hacking goes back just as far. Cyper often boasts about his affiliation to “Hackwieser”, a well-known hacking group founded in 1999.[19] Cyper also claims to be the ex-founder of “sleeperS crew”.

Cyper is also believed to be of the main individuals credited with the downfall of Hell Forum in 2015. According to someone close to the event, it is possible that the “Ping dox” incident, which caused the close of the Hell Forum, was orchestrated by Cyper as a way to steal the OPM data from Ping and launch his own forum, BlackBox.

TACTICS

Cyper takes great care in masking his language and has done so for years. He is extremely careful and meticulous and will often go out of his way to avoid sites with JavaScript (as he states often). Going as far back as 2015, user Cyper on Hell forum speaks with broken English.

Cyper will often alternate and interchange aliases and code samples with other colleagues in order to confuse security researchers and evade stylometric analysis. Most noteably, Cyper takes on the persona of "NSA" from WP. The handle NSA is now Cyper’s main handle on KA forum.

19 https://en.wikipedia.org/wiki/Hackweiser

4.5.1
HISTORY

In the late 1990s - early 2000s, threat actor Cyper was extremely active in the hacking community. Cyper made a name for himself by hacking and defacing hundreds of websites.

CyPeRtRoN's public defacements have been cached and can be viewed on Zone-H at: http://www.zone-h.org/archive/notifier=CyPeRtRoN/.

BRAGGING RIGHTS

Cyper regularly flaunts his history as a hacker and often reminds people of his accomplishments. In June 2015, Cyper made the following post on the original Hell forum bragging about an old hack / defacement of the U.S. Navy's website (navy.mil).

> *This is a CACHE (mirror) page of the site when it was saved by our robot on 2003-03-04 19:22:41*
> *btw is not important http://zonehmirrors.org/defaced/2003/03/04/owa.navseadn.navy.mil/Cy.jpg*
> *Glory days, huh? Well a lot has changed in 12 years.*
>
> *Mirror saved on: 2003-03-04 19:22:41*
> *Notified by: CyPeRtRoN*
> *Domain: http://owa.navseadn.navy.mil*
> *IP address: 207.132.146.227*
> *System: Win NT9x*

4.5.2

ATTRIBUTION

DETAILED ATTRIBUTION FOR TDO LEADER & KICKASS ADMIN

ATTRIBUTION SECTIONS

A. KickAss Forum Admin, NSA

B. Additional Cyper Aliases

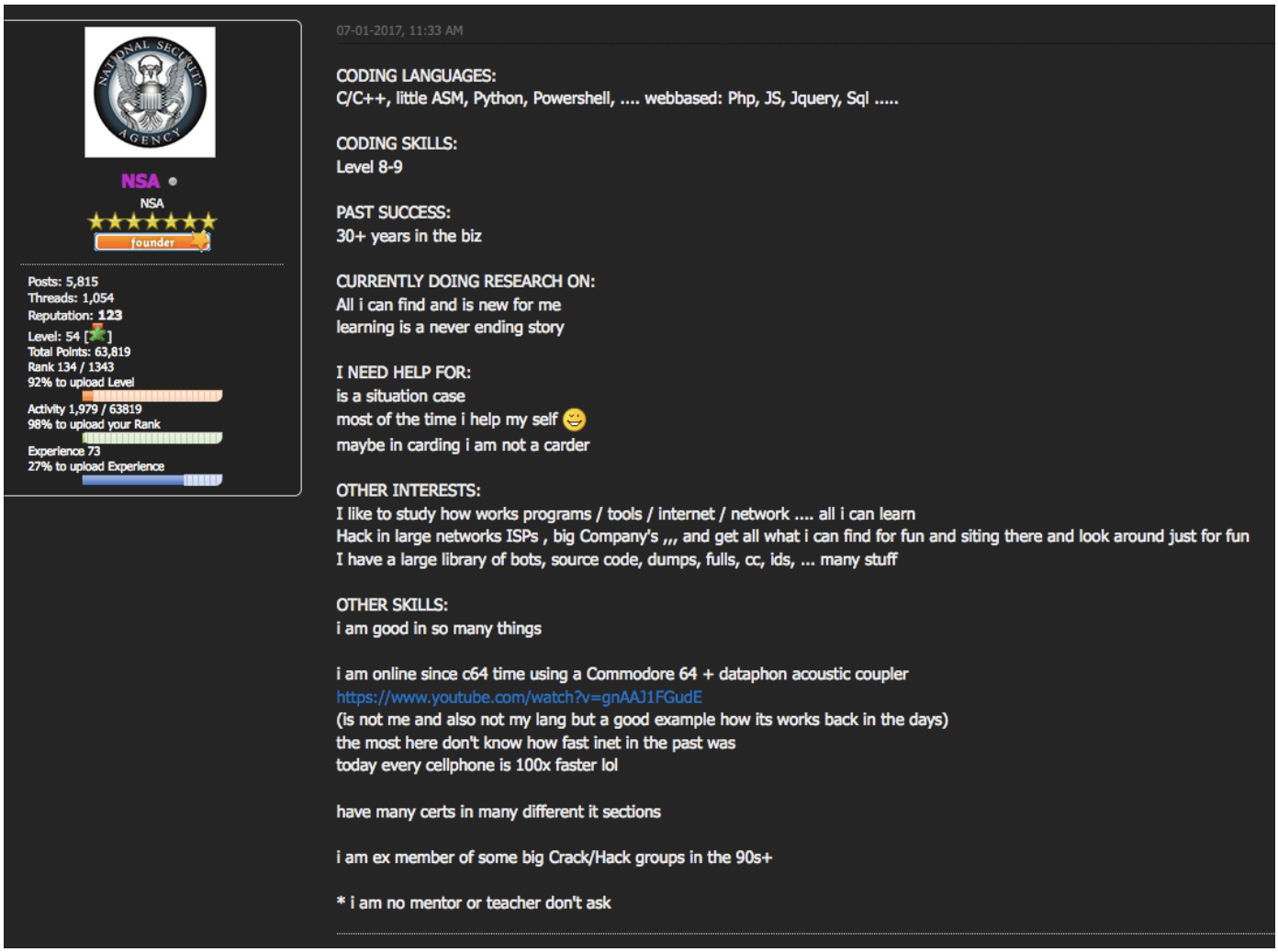
C. Hackweiser & Cyper's Origins

D. The Location of the KickAss Server

4.5.2.A

KICKASS FORUM ADMIN, NSA

NSA is the current admin/owner of the KickAss hacking forum. In the following post, NSA introduces himself and his skills. NSA mentions, “I am ex member of some big crack/hack groups in the 90s+”. NSA (Cyper) regularly refers to his affiliation with Hackweiser or SleeperS Crew.



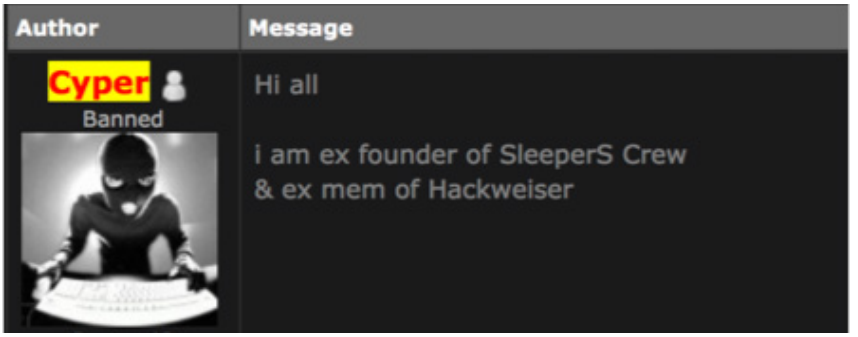
4.5.2.B

CYPER'S ALIASES

CYPER AND L00K

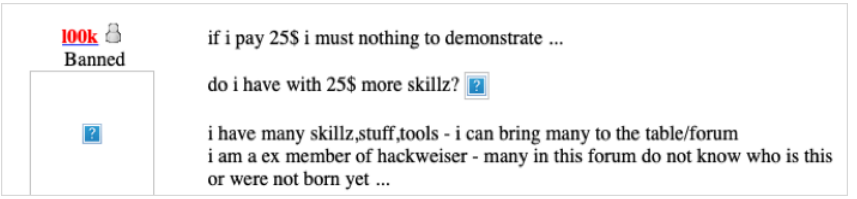
On forum 0day, users Cyper and l00k both introduce themselves has being ex-hackweiser members.

Cyper always introduces himself as the ex founder of SleeperS crew and an ex member of Hackweiser.



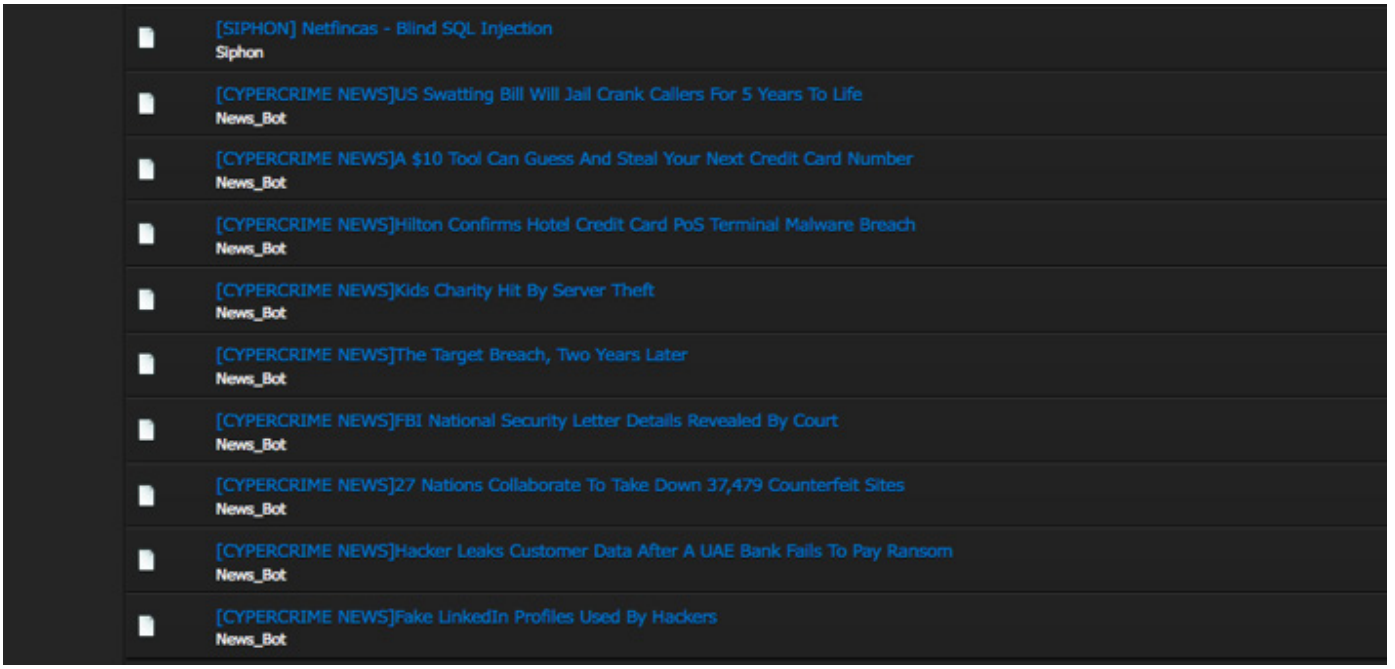
GHOST AND BLACKBOX

Following the demise of Hell, user Cyper and a small group of hackers moved over to BlackBox. Cyper was the known admin, under the name Ghost. The onion URL of BlackBox contained



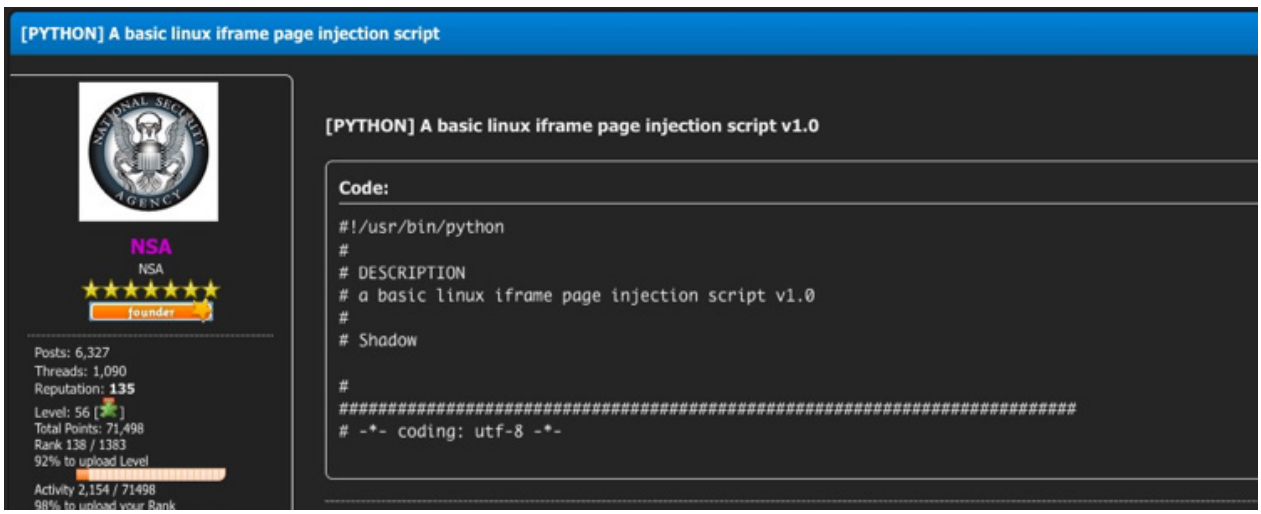
LINKING CYPER TO KICKASS

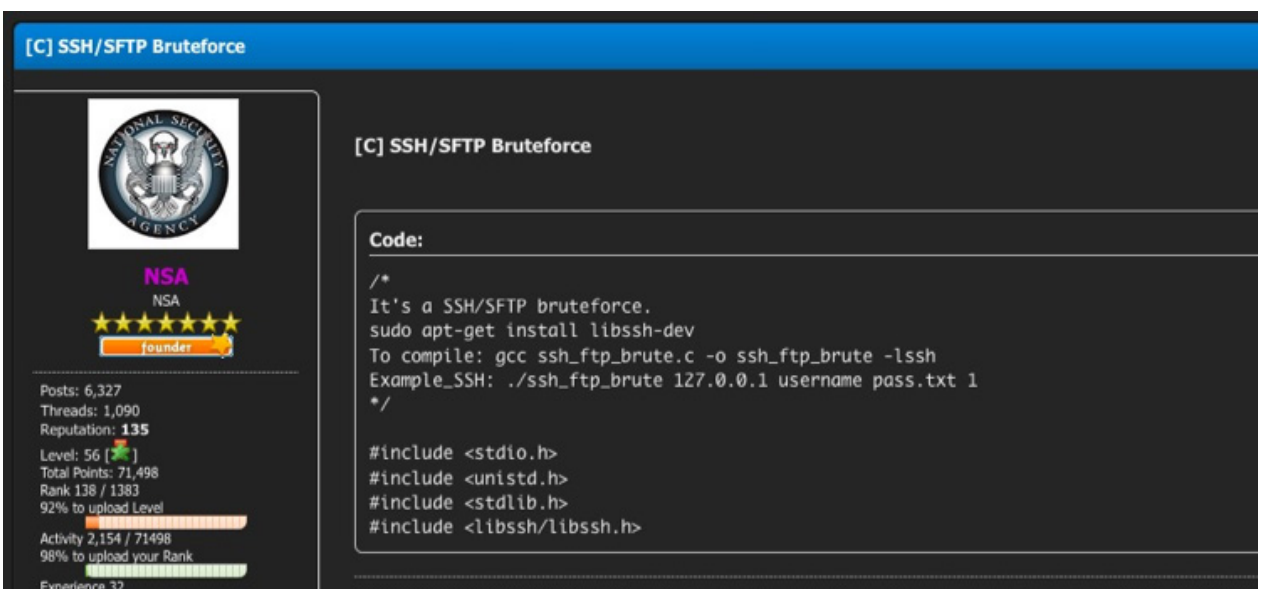
One sign that the KickAss forum belongs to Cyper can be seen in the forum's news posts. Initial news posts on the KickAss forum include the the word Cyper as part of a news gathering bot called "**Cyper**crime news".

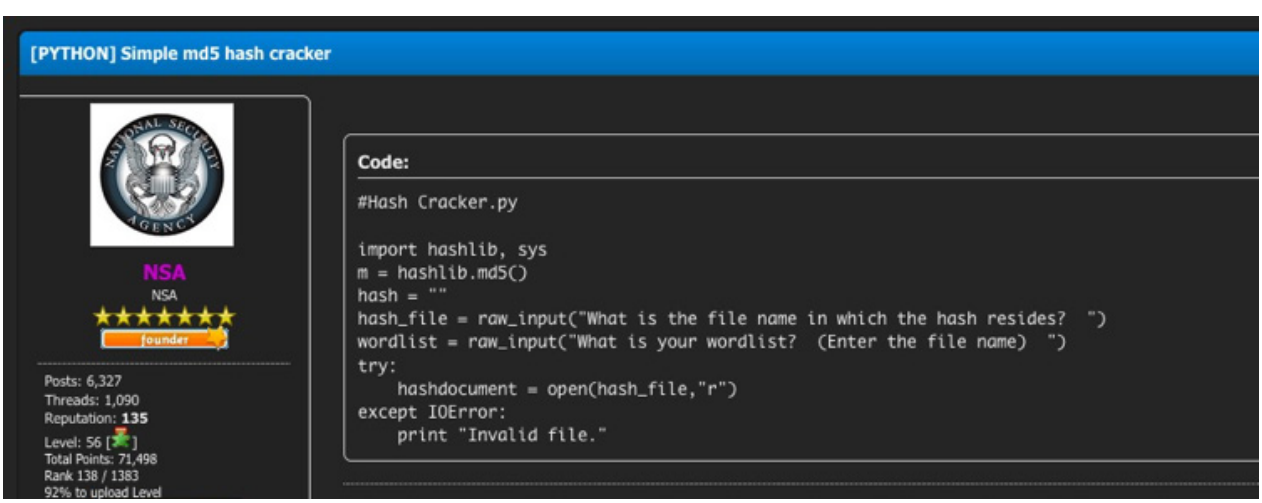


CODE SHARING WITH WP

On the KickAss forum, user NSA is currently in use by admin Cyper. However, Stylometry analysis confirms that several pieces of anonymous code published by NSA on forum KickAss were written by WP (the other NSA).







4.5.3.C

HACKWEISER: CYPER'S ORIGINS

On almost every forum introduction post, and whenever possible, Cyper brings up his affiliation to Hackweiser, a hacking group from the 90s.

GALAXY 2

On the Galaxy2 darknet social media site, user Cyper was again bragging about his affiliation with HackWeiser. In this thread, Arsyntex points out that Cypertron is in the members list:

> By CyPeRtRoN
>
> something to read for u https://en.wikipedia.org/wiki/Hackweiser
>
> By Arsyntex
>
> Members included; R4ncid, Bighawk, [P]hoenix, Immortal, RaFa, SquirrlIman, PhonE_TonE, odin, x[beast]x, Phiz, @CyPeRtRoN and Jak-away(AKA Hackah Jak).
>
> hahahaah (¬□¬)

WIKIPEDIA ARCHIVES

According to WikiPedia, the members included; R4ncid, Bighawk, [P]hoenix, Immortal, RaFa, SquirrlIman, odin, x[beast]x, Phiz, and Jak-away(AKA Hackah Jak) (with no reference to Cypertron).

The Wikipedia post revisions around that time reveal an edit where someone added Cypertron to the list of members. The IP address of **62.93.70.34** is a residential IP in Austria.

Hackweiser: Difference between revisions

From Wikipedia, the free encyclopedia

Browse history interactively

Revision as of 01:55, 27 November 2014 (edit)	Revision as of 11:10, 17 May 2015 (edit) (undo)
86.128.132.195 (talk)	62.93.70.34 (talk)
← Previous edit	Next edit →
Line 79:	Line 79:
Members included;	Members included;
− R4ncid, Bighawk, [P]hoenix, Immortal, [[RaFa]], SquirrlIman, PhonE_TonE, odin, x[beast]x, Phiz and Jak-away(AKA Hackah Jak).	+ R4ncid, Bighawk, [P]hoenix, Immortal, [[RaFa]], SquirrlIman, PhonE_TonE, odin, x[beast]x, Phiz, **CyPeRtRoN** and Jak-away(AKA Hackah Jak).
The group eventually fell apart and disbanded after the arrest of Hackah Jak in mid-2003.	The group eventually fell apart and disbanded after the arrest of Hackah Jak in mid-2003.

4.5.3.D

THE LOCATION OF THE KICKASS SERVER?

GALAXY 2 OPSEC FAIL

In 2016, on the Galaxy2 TOR social media forum, user @cyper and @arsyntex got into a heated argument with each other, apparently over who was the bigger 'noob'.

User @Sugartime jumped in with the following crucial information:

1. Rule of hidden services: Never speak of your real IP. #telnet cyper7cyb5re7u57.onion 25 Connected to cyper7cyb5re7u57.onion. 220 ks355296.kimsufi.com ESMTP Exim 4.84 Fri, 24 Jul 2015 xx:xx:xx +0200 #dig ks355296.kimsufi.com **91.121.120.49**

2. Rule of hidden services: For deniabilty, never speak Exim ident on your real IP. PORT STATE SERVICE VERSION 113/tcp open ident? #telnet **91.121.120.49** 113 Connected to **91.121.120.49**. 25, 25 : USERID : UNIX : fail 25,25:ERROR:NO-USER

At the time of writing this report in 2019, the IP address 91.121.120.49 is still associated with OVH hostname: ks355296.kimsufi.com. It would appear that the owner never changed the IP address.

4.5.4

SUMMARY

Summary of user Cyper, and his association to TDO

Cyper, aka Cypertron, is a seasoned hacker and C++ programmer. His history takes him as far back as the 90s, where hundreds of his hacks and public defacements are cached and can still be seen on www.zone-h.org.

Evidence suggests that Cyper was the figure that orchestrated the downfall of the original Hell Forum. Some actors close to the event suggest the event was a way for him to steal the hacked OPM data, which now rests behind an uncrackable RAR-hashed password. Regardless, Cyper use the downfall of the forum to launch his own hacking forums, KickAss and BlackBox.

BlackBox was an extremely private forum where only a few core members would assist each other with ongoing hacks, while KickAss was a semi-public forum used by the admins to scout new talent.

Cyper used the alias Ghost while admin of BlackBox, and NSA while admin of KickAss. Cyper's broken English and self-importance make him an easy target to spot.

As admin of both BlackBox and KickAss, it is also believed that Cyper was the core leader behind the original Dark Overlord hacking group.

Until its closure, the KickAss forum is used an exclusive forum for The Dark Overlord to sell their merchandise and promote their latest hacks.

Section 5

The Dark Overlord

Bonus Content

5.1

TIMELINE SUMMARY

2019

- U.S. authorities begin extradition of Nathan Wyatt for crimes related to TDO
- Authorities shut down XDedic marketplace
- KickAss forum closes in exit scam; fakes seizure notice and changes URL

2018

- BTC value crashes
- TDO recycles hacked data - most likely attempting to rebuild lost BTC value
- TDO re-surfaces. Begins campaign to promote data sale on KickAss forum
- KickAss Forum becomes private. Majority of old members purged
- KickAss membership fees skyrocket to $650

2017

- BlackBox forum closes with fake seizure notice
- 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

- TheRealDeal marketplace v2 launches
- Hell Reloaded launches
- KickAss forum launches
- BlackBox members form 'The Dark Overlord'
- Arnie and cr00k post medical data for sale on forums
- TDO extorts Netflix for $50,000
- TDO accesses major healthcare organizationss via RDP
- TDO gains access to additional orgs through HL-7 software
- W0rm rips off cr00k - cr00k dumps w0rm forum db
- Louisiana DMV Hacked - data sold by NSA
- 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
- Cyper launchs BlackBox forum as inner circle hacking forum
- TheRealDeal (v1) marketplace shuts down

5.2

A LATE NIGHT CONVERSATION WITH TDO

The following text is a small portion of the almost 4-hour conversation that occured 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.

5.3

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 begining 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 investiation.

For more information, visit www.dataviper.io