LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

HC3 Intelligence Briefing Update
The Dark Overlord

OVERALL CLASSIFICATION IS

UNCLASSIFIED

TLP:WHITE

5/2/2019

Agenda

The Dark Overlord

- Overview
- The Dark Overlord
- Campaign Strategies
- Social Media Marketing
- Recruitment Campaigns
- Notable Campaign Timeline
- Healthcare Targets
- School Targets
- 9/11 Files
- Arrests
- Mitigations
- Conclusions

Source: Fandom.com

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Overview

- The Dark Overlord (TDO) is an international cybercriminal group that has targeted the Healthcare and Private Health (HPH) sector, compromising hundreds of millions of health records since 2016.
- Is known for breaching organizations and demanding payment for the return of stolen data.
- Has been highly active in social media and news media, using these platforms as leverage to pressure organizations to pay ransoms.
- TDO has displayed significant technical ability in active campaigns, and seeks to recruit individuals who are proficient in cyber operations.
- The group has received notoriety due to attacks on many high profile organizations/targets.
- The criminal group focuses on targeting organizations that have a particular duty to safeguard client information, such as healthcare or law organizations.
  - Healthcare organizations must practice due care in maintaining a defense-in-depth approach against organizations who specifically target them.
  - It is also recommended that healthcare organizations contact the proper law enforcement agencies in the event of a breach, and <u>do not pay any ransom demands</u>

Source: fandom.com

The Dark Overlord

Source: Forbes, Bankinfosecurity

Who ~~is~~ Are The Dark Overlord?

- Self professed “Professional Adversarial Threat Group”
- International cybercriminal group whose current numbers are unknown
  - Originally thought to be an individual hacker.
- Has targeted a number of industries, including Healthcare, Education, Entertainment, and others.
- Primary motivation seems to be financially driven.
  - Focuses on breaching organizations to steal sensitive data, then attempts to coerce the target organization into paying a ransom
- Has been involved in cyber attacks on high profile targets
  - Includes Netflix, ABC Studios, U.S school districts, and Gorilla Glue
  - Surfaced in 2016 after a massive campaign, breaching a number of healthcare systems.
- Recently received attention in the media due to claimed theft of documents related to 9/11 attacks.
- Often, law enforcement officials are not sure if certain attacks are a result of TDO or copycats exploiting the group’s fame.
- Not to be confused with “The Dark Lord of the Internet”, Jesse Willms, accused fraudster.

Campaign Strategies

- From a technical perspective, TDO has exhibited a high degree of capability in executing cyber attacks, exploiting technical vulnerabilities, such as 0days in RDP protocols then escalating privileges to access critical information
- However, researchers have observed variances in how the criminal group conducts their campaign after a successful breach.
  - Earlier objectives seemingly involved simply selling stolen data on the dark web.
    - Conversely, researchers now believe the advertised data was simply to pressure the victim organization to pay a ransom.
  - TDO has privately corresponded with victim organizations after a breach, and has aggressively broadcasted attacks through social media and news.
  - The tone in which TDO interfaced with victims also displayed variances, ranging from friendly to visceral threats.
  - Through observed campaigns and interviews, researchers believe TDO is working on fundamentally improving how they extort payments from victims.
  - It also possible the variances in TDO interfacing may be due to different personalities within the group, or copycat individuals falsely claiming to be members of TDO.
- TDO often selects its targets based on the target's need to safeguard client data:

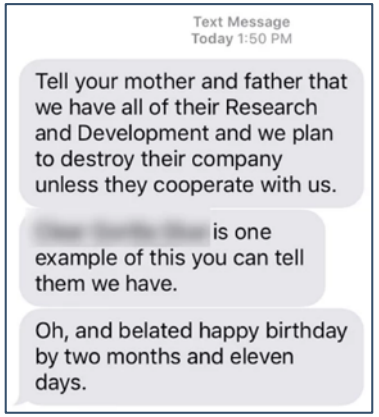
> *"Any organization that deals with sensitive personal information (e.g. medical institutions, law firms) is at a higher risk of being targeted and owes a particular duty of care to its clients because of the risk of severe emotional distress if client data is made public."*
>
> **- British National Cyber Security Center, in regards to TDO**

Source: Databreaches

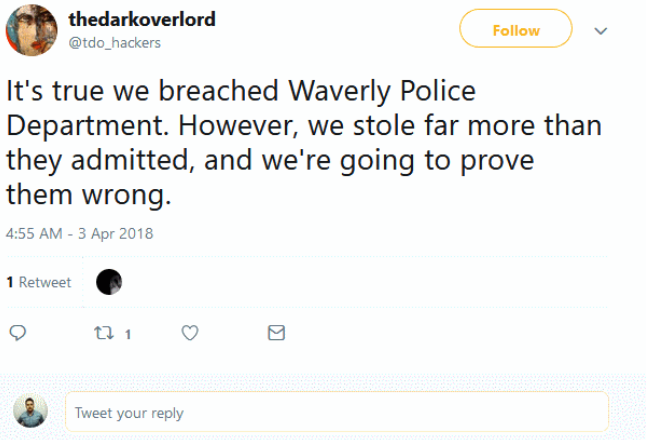
Social Media Marketing

- One of the key signatures of TDO is their level of presence on social media platforms, and direct interfacing with victims and news organizations during an active campaign.
  - Highly boisterous in their communication methods, TDO will often, taunt or joke with victims, and will also flaunt their abilities.
- The group has accepted interviews with several journalists/researchers in an effort to continue pushing their notoriety.
- Until recently banned from major social media platforms, TDO actively posted updates, highlighting ongoing and future activities.
  - TDO continues to look for other mediums to post content.
- To supplement an attack or breach, TDO will interface with targets directly to demand ransoms. TDO has been observed posting these conversations to social media.

  Observed campaigns indicated TDO will often escalate the publicity of an attack based on the cooperation of the target.



Alleged TDO text message
Source: Vice



Source: Bleeping Computer

Social Media Marketing

Publicly announced breach of a healthcare organization, posted via pastebin

text 2.97 KB raw download clone embed report print

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

This is thedarkoverlord (@tdohack3r) here to deliver a message.

We've recently had the pleasure of entertaining the company of an up-scale dentistry in the Manhattan area of New York City, after pillaging them and acquiring 3.5k patient records that contain both PII and PHI - unlike previous copycats. Yes, we know that 3.5k isn't a lot compared to our previous feats but we've decided to bring this breach to light due to the way we were treated by our target.

The name of this dentistry is none other than [redacted] located at [redacted]. They can be reached by phone at [redacted] and by email at [redacted]. Their website is [redacted]

Being the good-natured people we are, we contacted the dentistry after we had a copy of their patient records safely in our possession. After notifying them of this fact, we then proposed a course of action that would accomodate us both. However, for reasons unknown, they suddenly became hostile towards us and using very colourful language, foolishly declined (pictured on Twitter). However, after much contemplation, we've come to the conclusion that they may not be the most situationally-aware people. We understand that they'll require a gentle nudge or two which is why we'll still be giving [redacted] a choise to cooperate with us or suffer a stabbing pain inflicted by yours truly.

As proof that what we say is true, you will find below a link to sample of the data. Note that they contain PHI. Their records show that some patients have HIV, AIDS, Herpes Simplex, or Venereal Disease, and much more. More of these records specifically will be released if [redacted] does not cooperate with us.

As always, we are open to communication and discussion with all of our valued business partners.

Here is a link to sample records: http://pastebin.com/LVUwHFr8

Until next time,
thedarkoverlord
Professional Adversary
World Wide Web, LLC

This message is PGP signed so you can verify its authenticity. You can find our PGP key and fingerprint on our Twitter.
-----BEGIN PGP SIGNATURE-----
```

Source: Pastebin

Recruitment Campaigns

Source: Cyberscoop

"Do YOU want to get Rich? Come work for us!"
– The Dark Overlord

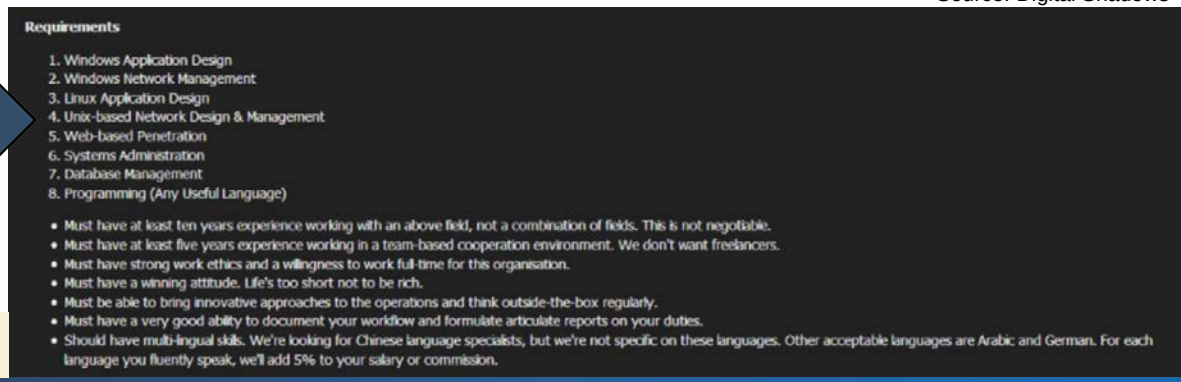
- In an effort to bolster it's numbers, TDO has been observed posting recruitment advertisements on popular hacker forums.
  - Job requirements included experience with Windows, Linux as well as expertise in Unix-based design and network management and penetration testing.
  - New employees would be paid 50,000 pounds ($63,500) monthly, plus add-ons and a likely pay bump up to 70,000 pounds ($89,000) monthly after two years.

Job Summary:

"You'll be working in a strong team-based environment, communicating and collaborating with like-minded and ambitious individuals. You'll be checking into project trackers, accepting suitable workflow positions, and carefully documenting your work for review. You'll be engaged in operations against various companies and governments and world-wide deployments. If you're goal-oriented and used to objectives and achieving them, then you're perfect for us."

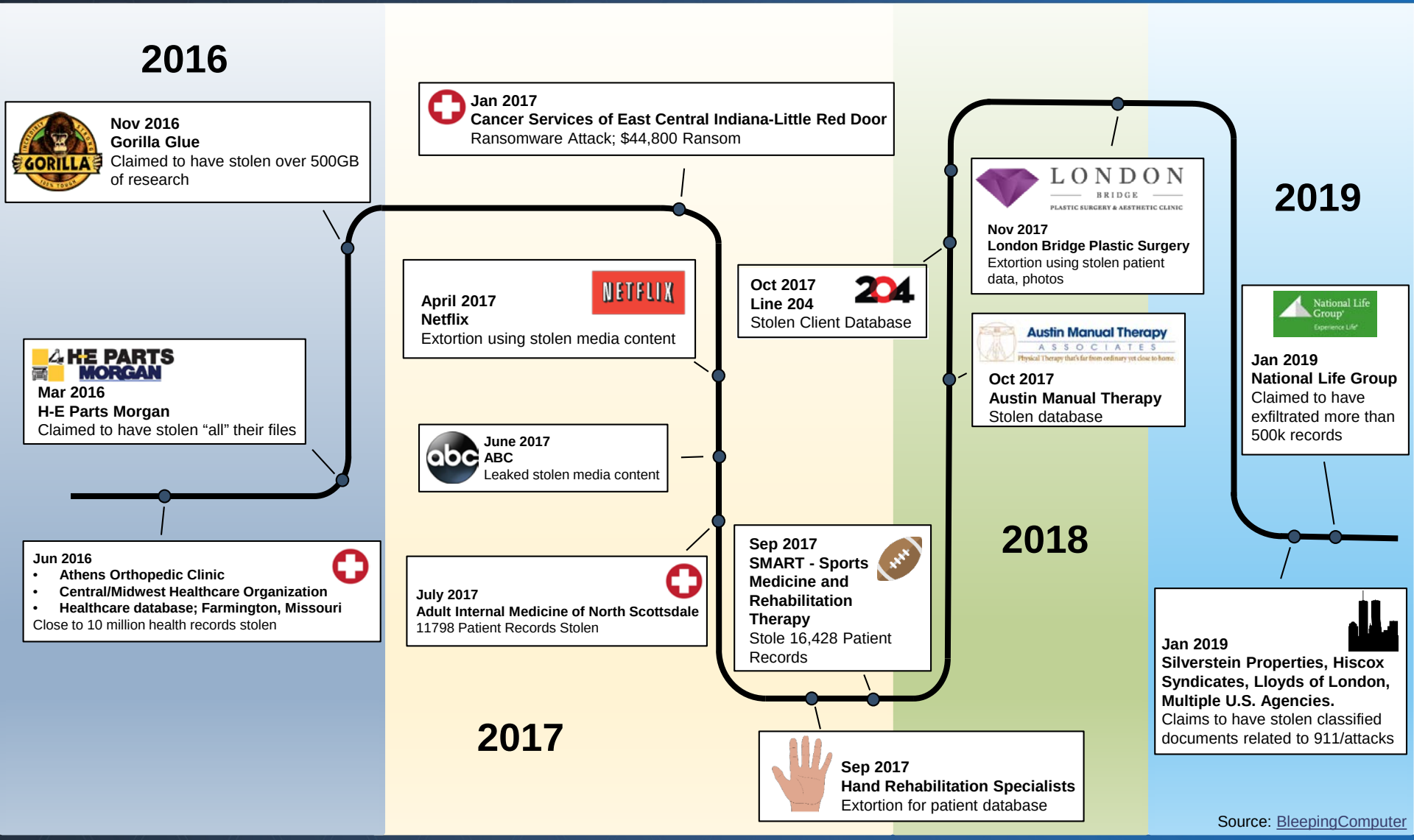
Source: Digital Shadows

Job Position Requirements



"Must have a winning attitude"

Notable Campaign Timeline



Source: BleepingComputer

Healthcare Targets

Source: Miami Herald, idigitalhealth

- Being financially motivated, TDO views the healthcare sector as a highly profitable target group.
  - Healthcare obligations to protect PHI data add further leverage to ransom demands
- The theft of up to 10 million health records was one of the first campaigns that lead to TDO notoriety in 2016.
  - Since 2016, TDO has been connected to breaches on a plethora of healthcare organizations, resulting in hundreds of millions of stolen records.
- TDO has focused on targets of opportunity, attacking a variety of organizations within healthcare
  - Hospitals, EHR systems, health insurance firms, charity organizations, etc.
- TDO has also been observed selling massive amounts of stolen PHI on the dark web for profit, pressuring the victim health organization to pay a ransom
- In Jan 2019, the group attacked London Bridge Plastic Surgery to obtain medical information on high-profile celebrities.

School Targets

Source: Washington Post, CSOonline

- The Dark Overlord has been observed attacking schools in a variety of campaigns.
- In Oct 2017, TDO targeted the Johnston Community School District in Iowa.
  - Information contained student names, addresses and telephone numbers.
  - Data was compromised through a third party vendor that works with the school district.
  - TDO released personal information on students – making it easy for "any child predator to easily acquire new targets".
  - Using the hacked credentials, TDO sent out mass threats to students and parents.
    - Then posted received voicemails and texts of victim responses.

"I'm going to kill some kids at your son's high school,"
- The Dark Overlord

  - TDO has also taken credit for a on the Splendora Independent School District in Texas, demanding a ransom for student personal information.
  - Hacking in Montana Columbia Falls School District – sent a 7 page ransom letter demanding $75,000 in bitcoin in exchange for not releasing student information.
  - Schools in Crenshaw County, AL were shut down after the FBI warned country officials of alarming social media threats by TDO.
- TDO attacks prompted The Department of Education to released a warning advisory in regard to this new cyber threat against school districts.

"We're escalating the intensity of our strategy in response to the FBI's persistence in persuading clients away from us."

- The Dark Overlord, during a Daily Beast interview when asked, "why attack schools and threaten kids?"

9/11 Files

- In January of 2019, TDO claimed to have stolen highly sensitive documents related to the 2001, September 11th attacks.
  - Claimed to have stolen the information from insurers Hiscox Syndicates Ltd and Lloyds of London, and real estate developer Silverstein Properties.
  - Also claimed to have taken the information from U.S. agencies, including the FBI, the Department of Justice, the Federal Aviation Administration and others.
- TDO released a sample of the files with access instructions and a decryption key.
  - The documents refer to liability cases regarding the World Trade Center attacks.
- Other files will be release a possible five installments in exchange for cryptocurrency.
  - TDO is offering the documents, which it claims are at the Top Secret Level for two million in bitcoin
  - The cheapest release will be sold for $5,000 in bitcoin.
- The bitcoin wallet where the group is asking for payment has received 34 transactions and has received around $18,000 so far.

Image source: Wikipedia

"If you're a terrorist organisation such as ISIS/ISIL, Al-Qaeda, or a competing nation state of the USA such as China or Russia, you're welcome to purchase our trove of documents."

- The Dark Overlord, via pastebin

Source: Cyberscoop, Bankinfosecurity

Arrests

- In 2017, Nathan Wyatt, aka “Crafty Cockney” was arrested in UK, pleading guilty to 20 counts of fraud, two counts of blackmail and on count of possession of a identity document with intent to deceive.
  - Used malware to steal files from a British Law firm and ransomed for $12,000 in bitcoin
  - Signed all ransom notes with “The Dark Overlords”
  - Claimed to be planning to call and shake down an unnamed Georgia clinic - potentially the Athens Orthopedic Clinic - on behalf of The Dark Overlord .

Nathan Wyatt Photo
Source: London Metropolitan Police Service

- Was release from jail in 2019, is currently fighting extradition charges from the U.S.
- In an interview, spoke about working with the TDO
  - Admitted to working with TDO member to teach them fraud techniques
  - Also discussed being asked by TDO to make a extortion phone call to a U.S. victim.
- Police found evidence that Wyatt had used his own details and live-in partner’s details to set up bank accounts in the U.K. to funnel payments to TDO from U.S. medical entities that TDO was attempting to extort at the time.

- In 2018, Serbian law enforcement, in cooperation with the FBI, arrested a 38-year-old man in Belgrade with the initial S.S., believed to be tied with TDO
  - The arrest was part of a larger campaign aimed at pursuing members of the organization.

Source: Axios, Databreaches, Cyberscoop

Mitigations

- Although it is impossible to ascertain every technique criminal groups like TDO will utilize to compromise an organization, there are a number of recommended best practices that can be adopted for a defense-in-depth approach:
  - Deployment of proper network security controls such as firewalls and content filtering software.
  - Utilizing endpoint security software such as antivirus suites and disk encryption
  - Ensuring proper training and awareness procedures are in place for personnel.
  - Using applications whitelisting to index and permit approved software
  - Applying the principle of least privilege to administrative accounts.

- In the event of a breach, we **do not** recommend paying a ransom if demanded.
  - We suggest contacting local law enforcement in the case of a cyberattack. The FBI's internet Crime Complaint Center (ICS) can be reached here: https://www.ic3.gov/complaint/default.aspx/

Source: Datebreachtoday

Conclusion

Upcoming Briefs

- Credential Stuffing

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide their feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**