



FireEye®



Disruptive Breaches

Real World Cases of Theft, Extortion,
Destruction and Public Shaming

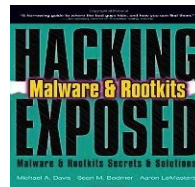
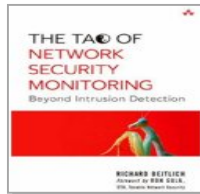
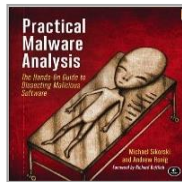
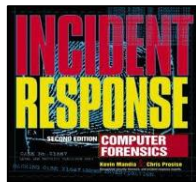


PRESENTED BY: **CHARLES CARMAKAL** | VICE PRESIDENT

Background

Mandiant / FireEye

- Focused on mitigating, detecting, and recovering from security breaches
- Respond to hundreds of sophisticated breaches every year
- Knowledge of thousands of threat actors operating across the globe



Charles Carmakal

- Vice President, Mandiant
- Based in Washington DC
- Leads a team of incident responders that has responded to over a thousand incidents
- 18+ years of experience with incident response and red teaming
- Previously led the security consulting business at a Big 4 consulting firm

Agenda

- Threat actor motivations and capabilities
- Details of real world attacks
- Lessons learned from responding to disruptive breaches



**THE RULES OF ENGAGEMENT HAVE CHANGED -
THREAT ACTORS WILL CONTINUE TO INCREASE THEIR AGGRESSION**





RUSSIA

Disinformation Campaign (2016)

- Attempted to influence public opinion on the Syrian conflict, NATO-Ukraine relations, the U.S. presidential election, and the 2016 Olympics and Paralympics
- Have appropriated a pre-existing hacktivist or political brand in order to:
 - Obfuscate the true origin and identity of the operators behind the personas
 - Take advantage of the existing preconceptions about these brands
- Direct advocacy with victim, media, general public through social media



DC
LEAKS

GUCCI
FER2.0



ANONYMOUS



Case Study: Stealing Emails of U.S. Politicians

From: Google <no-reply@google.support>
Date: [REDACTED] 2016 at [REDACTED] PM
To: [REDACTED]
Subject: Your account is in danger



Hi

Our security system detected several attack attempts on your Google account. To improve your account safety use our new official application "Google Scanner".

[Permit Scanning](#)



Best, The Mail Team

2016 Mail Corp. 1677 Amphitheatre Parkway, Mountain View, CA 92042

Case Study: Stealing Emails of U.S. Politicians

From: Google <no-reply@google.support>
Date: [REDACTED] 2016 at [REDACTED] PM
To: [REDACTED]
Subject: Your account is in danger



Hi

Did not address the recipient's first name

Our security system detected several attack attempts on your Google account. To improve your account safety use our new official application "Google Scanner".

[Permit Scanning](#)

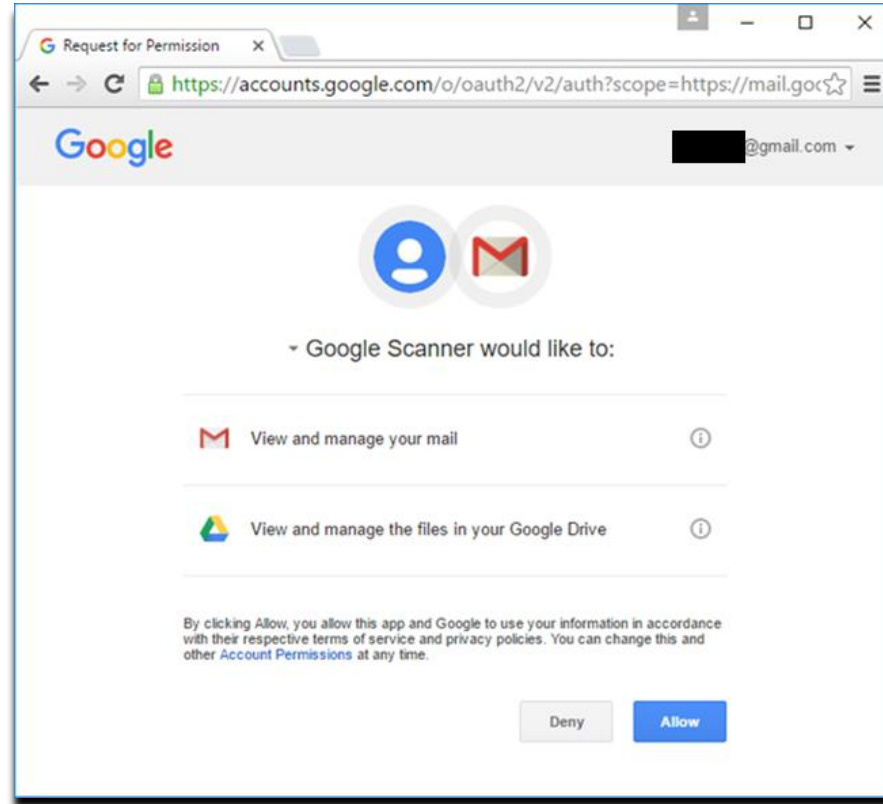
Linked to <http://bit.ly> shortened address



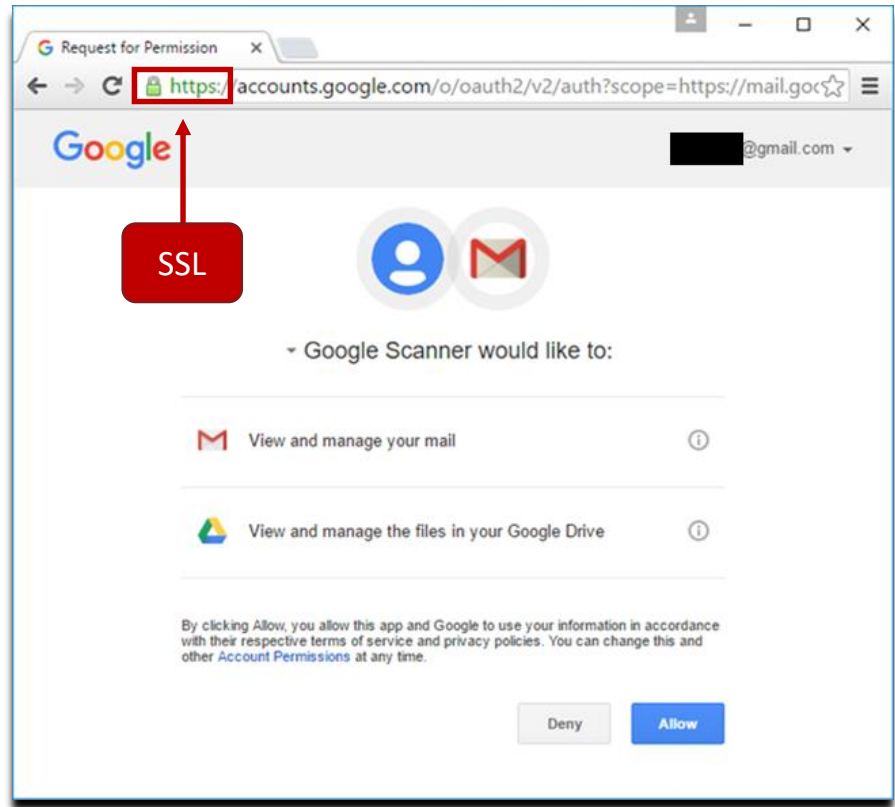
Best, The Mail Team

2016 Mail Corp. 1677 Amphitheatre Parkway, Mountain View, CA 92042

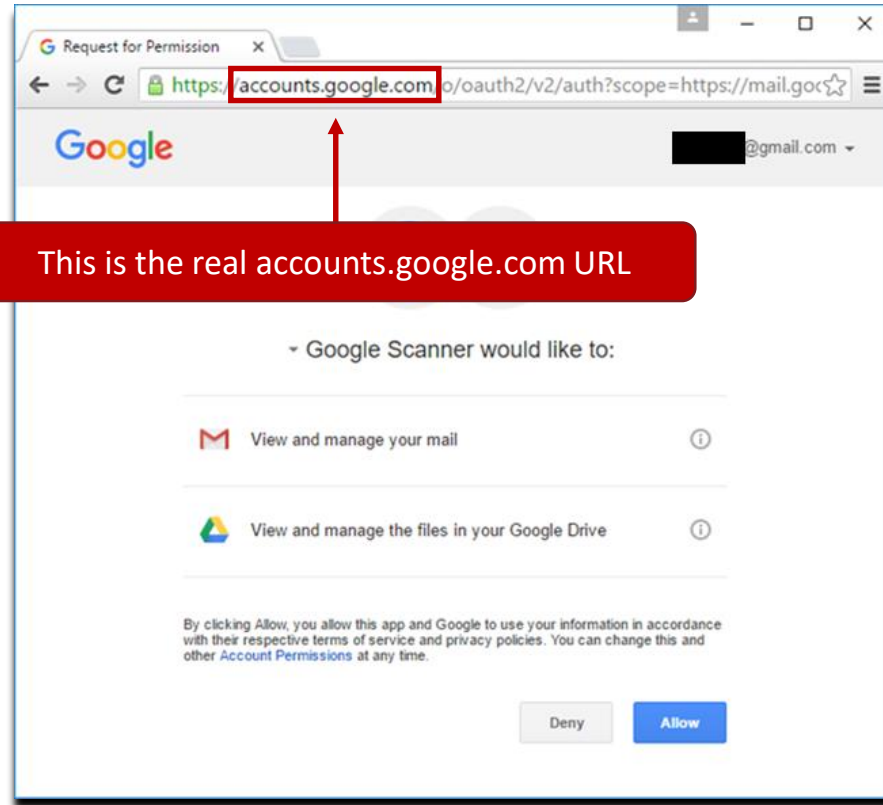
Case Study: Stealing Emails of U.S. Politicians



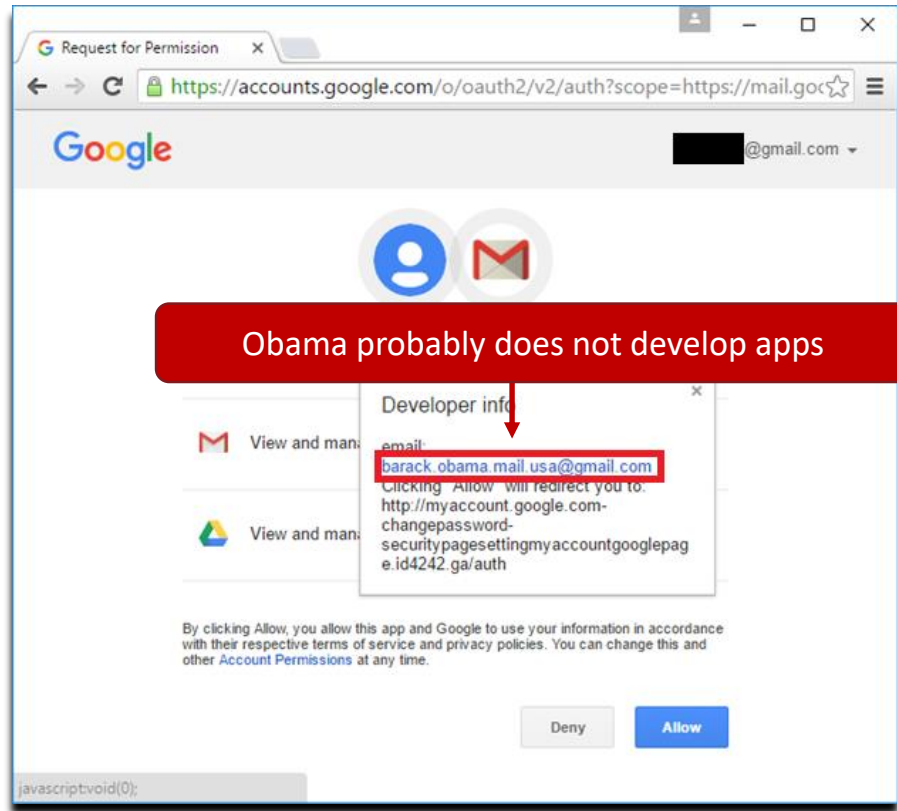
Case Study: Stealing Emails of U.S. Politicians



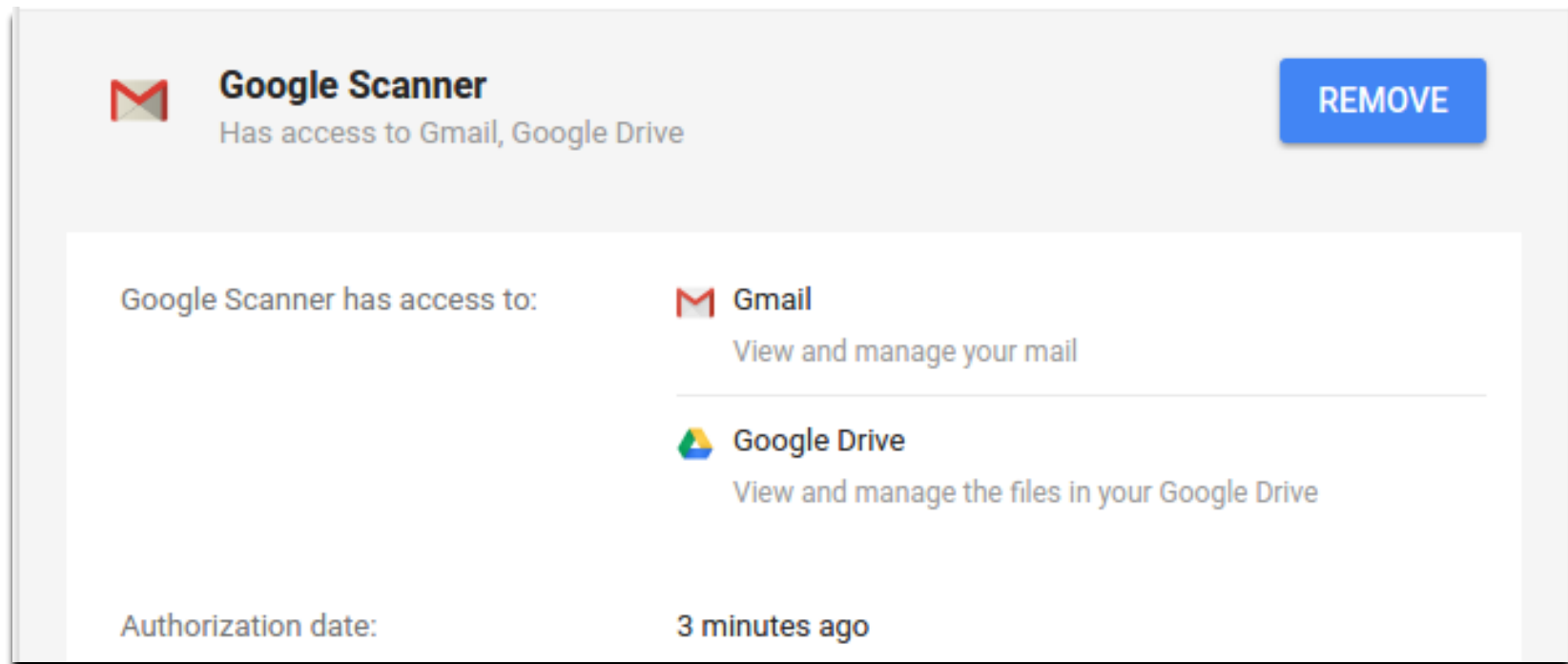
Case Study: Stealing Emails of U.S. Politicians



Case Study: Stealing Emails of U.S. Politicians



Case Study: Stealing Emails of U.S. Politicians



The screenshot shows a Google account access management interface. At the top left is the Gmail icon and the text "Google Scanner" with a subtext "Has access to Gmail, Google Drive". A blue "REMOVE" button is in the top right. Below this, a section titled "Google Scanner has access to:" lists two permissions: "Gmail" (with a subtext "View and manage your mail") and "Google Drive" (with a subtext "View and manage the files in your Google Drive"). At the bottom left, it says "Authorization date:" followed by "3 minutes ago" on the right.

Google Scanner
Has access to Gmail, Google Drive **REMOVE**

Google Scanner has access to:

- Gmail**
View and manage your mail
- Google Drive**
View and manage the files in your Google Drive

Authorization date: 3 minutes ago

“Ransomware” Against Ukraine in June 2017

- On June 27, 2017, a suspected Russian threat actor launched a wide-scale attack against Ukraine
- The attack was masked as a financially-motivated ransomware operation
- True intention was likely to disrupt business operations and impact the way of life in Ukraine
- Threat actor compromised the systems of a major provider of tax software and pushed a malicious update
- The update propagated across company networks and encrypted hard drives
- Downstream impact to several multinational organizations who do business in Ukraine

```
Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:
████████████████████████████████████████████████████████████████████████████████

2. Send your Bitcoin wallet ID and personal installation key to e-mail
wousmith123456@posteo.net. Your personal installation key:
████████████████████████████████████████████████████████████████████████████████

If you already purchased your key, please enter it below.
Key:
```

IRAN

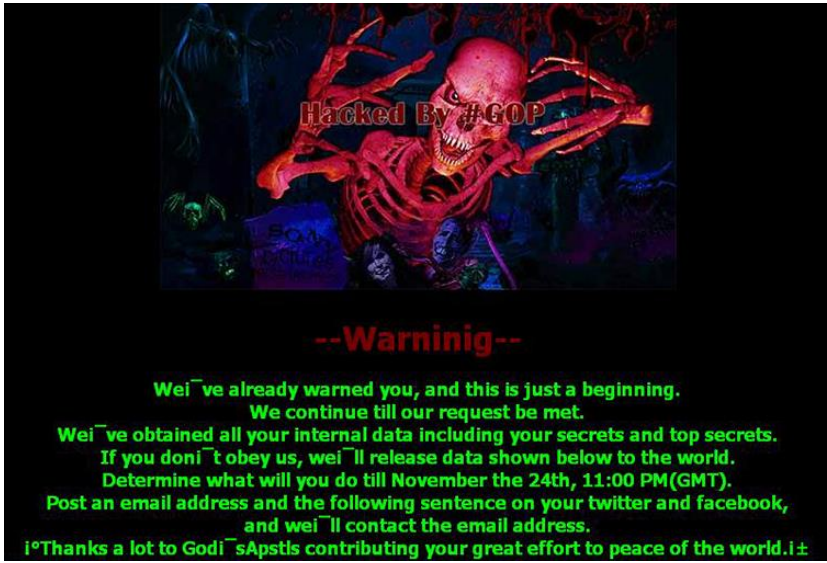




NORTH KOREA

Guardians of Peace vs. Whois Team (Dark Seoul)

US-based Entertainment Company



South Korean Media and Banks in Prior Year



Robbing the House, then Burning it Down

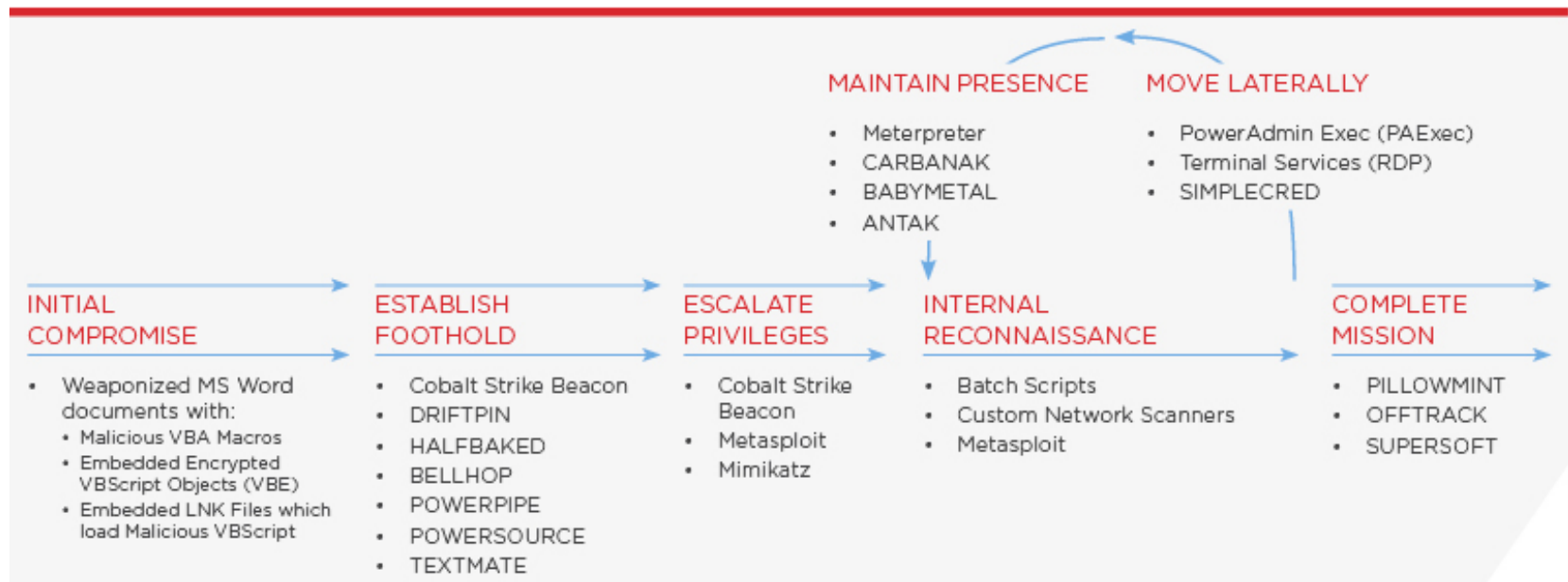




ORGANIZED CRIME

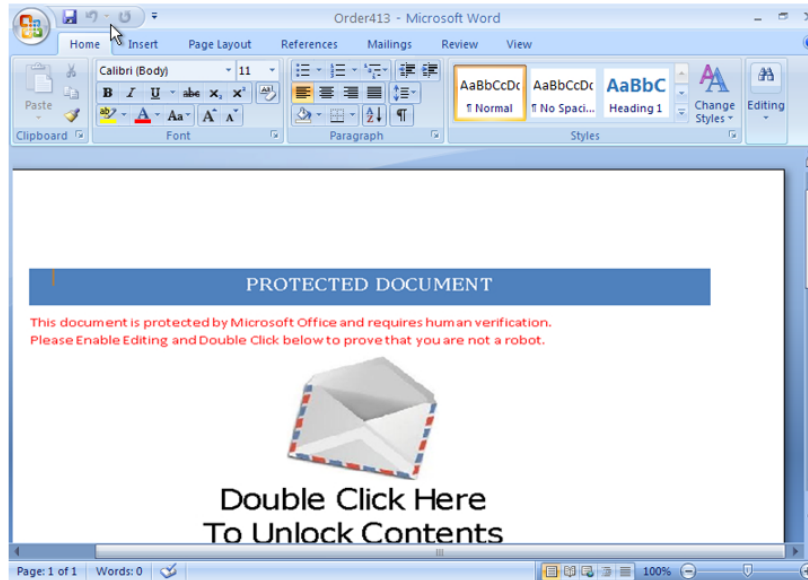
Threat Actor Overview: FIN7

- FIN7 is one of the world's most prolific financially motivated threat actors
- They conducted operations against hundreds of organizations since at least 2015



FIN7 Phishing Lures

- FIN7 often contacted victims over the phone prior to sending phishing emails and again afterward to help them open malicious attachments.



XML-formatted attachment (DOCX) with an embedded Object Linking and Embedding (OLE) object



DOCX and RTF files with an image that spawns a hidden embedded malicious LNK file when the image is double clicked

FIN7 = Combi Security

- On August 1, 2018, the DOJ unsealed an indictment against three Ukrainian nationals:
 - Dmytro Fedorov, 44
 - Fedir Hladyr, 33
 - Andrii Kolpakov, 30
- They used a front company named Combi Security to recruit "penetration testers"
- Advertised offices in Israel, Russia, and Ukraine
- Combi Security listed multiple U.S. victims among its purported clients
- Like any company, they have A-team players and D-team players





INDUSTRIAL SABOTAGE

Compromise of Safety Control System: TRITON (2017)



Facts

- Unexpected (but safe) plant shutdown triggered investigation
- Threat actor was able to inject custom code to the Triconex controller
- Attacker compromised and maintained remote access to various OT hosts, including the DCS and a legitimate engineering workstation

Attribution and analysis

- Nation State (moderate confidence)
- Attacker didn't likely intend to cause disruption at the time of the incident (versus long-term)



EXTORTIONISTS

FIN10 - Disrupting Mining Operations

- Threat actor called themselves “Tesla Team” (Mandiant calls them FIN10)
- Relatively unsophisticated threat actor, but very disruptive and destructive
- Compromised multiple natural resources and casino organizations in Canada
- Created scheduled tasks to destroy production systems across the enterprise
- Extorted victims to pay ransoms between \$50K and \$620K (in Bitcoin)
- Victims endured system outages for multiple days as they recovered data from backups



FIN10 - Disrupting Mining Operations

- The real TeslaTeam is believed to be a Serbian hacking group known for DDoS and defacement
- They are unlikely to be targeting Canadian organizations
- The threat actor previously claimed to be a Russian hacking group – “Angels of Truth”
- Likely use of Google Translate to write in Russian



The Dark Overlord – Extortion and Death Threats

- Has operated since at least 2016, but likely earlier.
- Modus operandi: Steal data and extort businesses
- Relatively unsophisticated threat actor – buys credentials or brute forces credentials where RDP is exposed to the Internet
- Recently targeted schools and sent death threats to students and parents



Lessons learned

1. Confirm there actually is a breach
2. Human adversary
3. Timing is critical
4. Stay focused
5. Carefully evaluate whether to engage attacker
6. Engage experts before a breach (forensic, legal, public relations)
7. Consider all options when asked to pay ransom/extortion
8. Ensure strong segmentation and control over backups
9. After the incident has been handled, immediately focus on broader security improvements
10. If you kick them out, they may try to come back



FireEye®

Questions?

Charles Carmakal

Vice President

charles.carmakal@mandiant.com

+1 864 735 7242

<https://www.linkedin.com/in/charlescarmakal>