INGUARDIANS™

CYBER SECURITY IS OUR SHARED RESPONSIBILITY

WHAT ARE WE DEALING WITH

AND

WHAT DO WE NEED TO DO?

NORTH DAKOTA CYBER SECURITY CONFERENCE

Jay Beale, CTO and COO at InGuardians

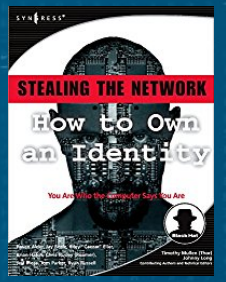
@jaybeale and @inguardians

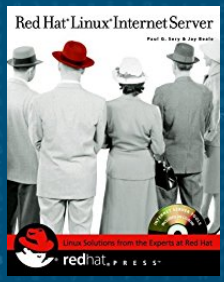
March 15th, 2018

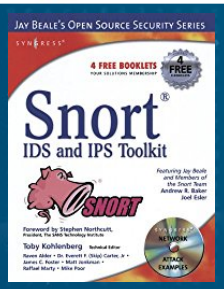
https://www.InGuardians.com

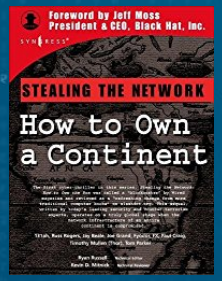
Check Twitter for my notes pages with links

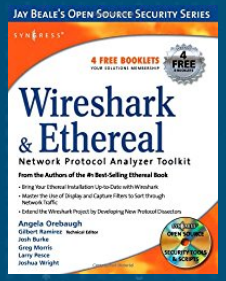
My Graphical Bio

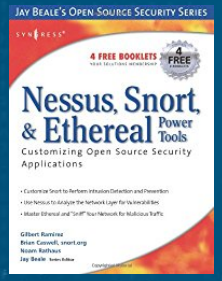


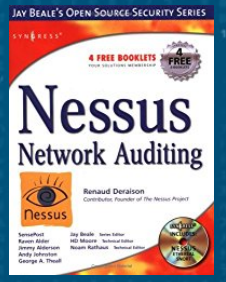


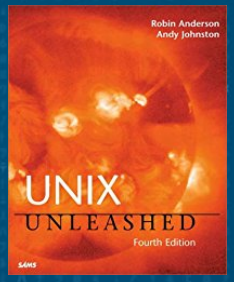












2017 Brought Internet Worms Back

- To many, it seems like we haven't had a "real" worm since 2008 with Conficker.
- Conficker used MS08-067, one of the last "weapons grade" SMB exploits to be publicly available.
- The public rarely sees reliable SMB-targeted remote code execution exploits.
  - Governments and criminals buy and hide these.
- WannaCry and NotPetya used one of the government-hidden weapons grade exploits, ETERNALBLUE, leaked by the Shadow Brokers.
- Other worms used ETERNALBLUE, including EternalRocks, which used seven exploits leaked by the Shadow Brokers.

WannaCry

- May 12-15th, 2017
- Ransomware
- Lasted only three days, because of a kill switch.
- 230,000 or more systems infected.
- Incredibly detrimental to the UK's National Health Service.
- Patches were two months old.

INGUARDIANS™

North Korea’s Lazurus is Mature and Active

- Both the US and the UK have attributed WannaCry to the Lazurus Group.
- Lazurus’s past operations:

1

Troy operation

Period: 2009-2012
Target: cyber espionage agaist armed forces and governmental bodies of South Korea, sabotage.
Method: hacking websites, stealing information, DDoS-attacks.

2

DarkSeoul operation

Period: March 2013
Target: three broadcasting stations, a bank in South Korea.
Method: infecting with viruses, stealing and wiping information.

3

Attack on Sony Pictures

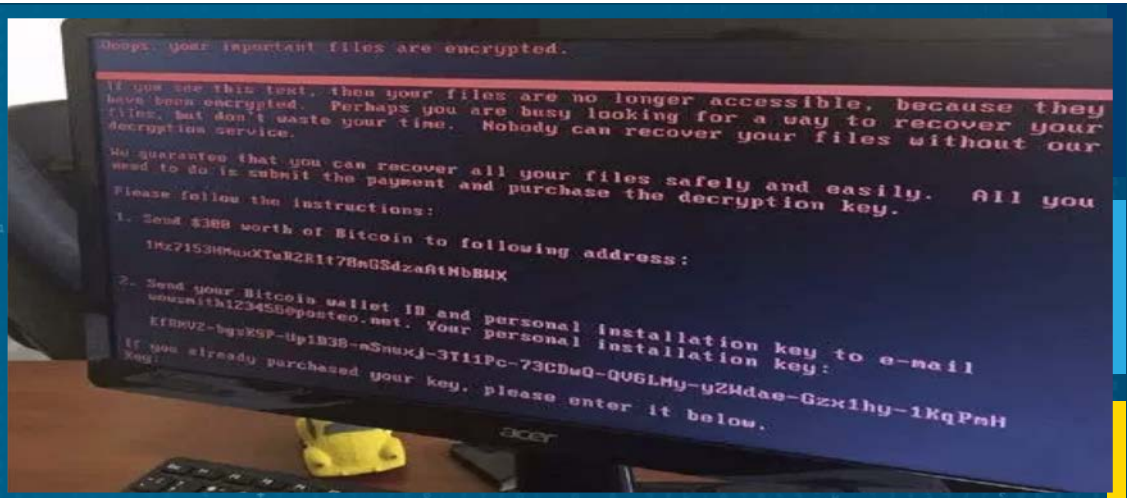
Period: November 2014
Target: Sony Pictures Entertainment (released the "Interview" movie, ridiculing the North Korean leader).
Method: infecting with malware, stealing and wiping data of the company's employees, correspondence, copies of unreleased films.

4

Attack on the Central Bank of Bangladesh

Period: 2016 year
Target: an attempt to steal $951 from the Central Bank of Bangladesh. Managed to steal only $81 million.
Method: a targeted attack on the system of interbank transfers SWIFT.

NotPetya



- June 27, 2017
- Targeted at, but not restricted to, Ukraine.
- First distribution point was likely a compromised MeDoc update server.
  - MeDoc's software was installed on roughly 1 million computers in the Ukraine.
  - MeDoc had roughly 400k clients, 90% of the domestic firms.
- Radiation monitoring systems at Chernobyl went offline.
- Appeared to be ransomware, but turned out to be wiperware.

NotPetya Attribution: GRU's Fancy Bear

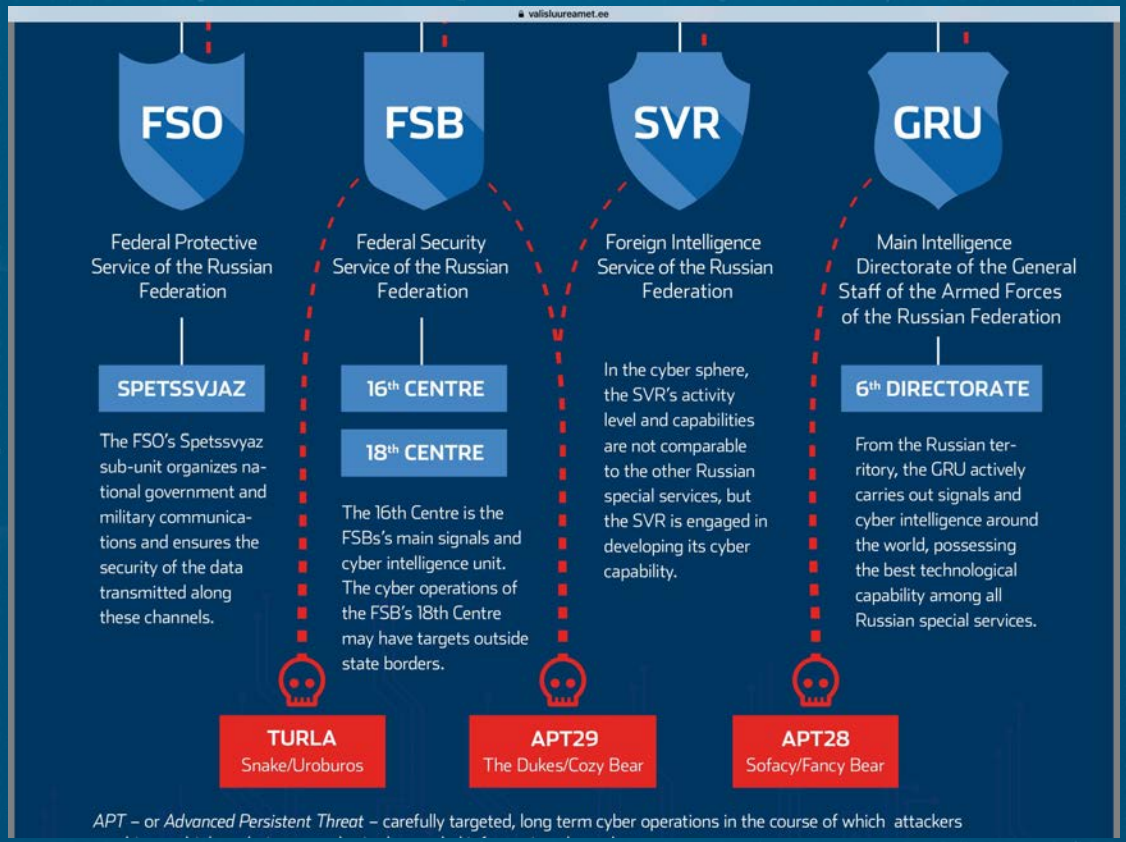
- The GRU military spy agency created NotPetya, the CIA concluded with "high confidence" in November, according to classified reports cited by U.S. intelligence officials. (January 12, 2018)

- "The UK Government judges that the Russian Government, specifically the Russian military, was responsible for the destructive NotPetya cyber-attack of June 2017," said Foreign Office Minister Lord Ahmad in a statement published online a few minutes ago. (February 14, 2018)

Fancy Bear's Other Attacks

- Fancy Bear - has attacked:
  - the German parliament,
  - the French television station TV5Monde
  - the White House,
  - NATO
  - the Democratic National Committee
  - Organization for Security and Co-operation in Europe
  - the campaign of French presidential candidate Emmanuel Macron

Russia's Cyber Hacking is Mature and Aggressive



Wiperware

- "We believe the ransomware was in fact a lure to control the media narrative, especially after the WannaCry incidents to attract the attention on some mysterious hacker group rather than a national state attacker like we have seen in the past in cases that involved wipers such as Shamoon. The fact of pretending to be a ransomware while being in fact a nation state attack -- especially since WannaCry proved that widely spread ransomware aren't financially profitable -- is in our opinion a very subtle way from the attacker to control the narrative of the attack."

Matt Suiche, Comae Technologies

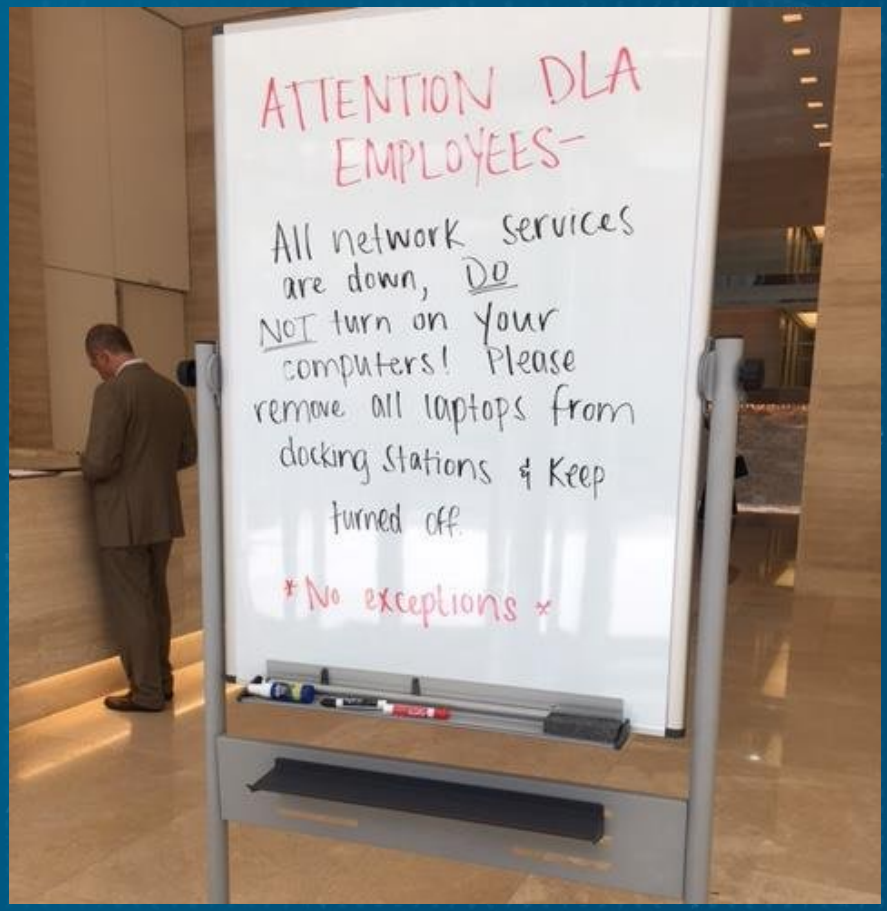
Damage Estimates from NotPetya

Fedex	$300 million	
Moller-Maersk (Shipping)	$275 million	
Mondelez (Cadbury)	$150 million	
Reckitt Benckiser (Pharma)	$132 million	
Saint Gobain (Construction)	$114 million	(extrapolated)
Beiersdorf (Nivea Skin Cream)	$41 million	
Nuance Communications	$15 million	

These numbers are solely for the publicly-reported losses.

Computers Off, Pencils Down

- This is what a ransomware worm outbreak looks like to a firm's employees, at best.



What Made NotPetya More Dangerous?

- We've seen worms spread by SMB before, using an SMB exploit
  - These often rely on every target system having the same vulnerability.
- NotPetya spread like a low-quality internal network penetration test.
  - Mimikatz – find passwords and hashes in memory
  - PSExec and WMI – run commands and programs (itself) on a remote system
- "The only component that looked sophisticated, finished, and ready to go, was the network propagation module, … NotPetya's authors were more interested in making sure the ransomware reaches as many people as possible."

NotPetya's Sequel: Bad Rabbit

- Bad Rabbit hit the scene in October of 2017.
- Initial infections occurred via a fake Flash player update "drive by" attack.
- Bad Rabbit then spread using Mimikatz to lift passwords from machines, adding these to a brute force list, which it used to propagate.
- It did not use EternalBlue.
- Bad Rabbit appears to be the work of the same group as NotPetya.

Bad Rabbit's Victims

- Odessa airport in Ukraine
- Kiev subway system in Ukraine
- The Ministry of Infrastructure of Ukraine
- Three Russian news agencies

What about crypto-mining?

Isn’t ransomware so yesterday’s news?

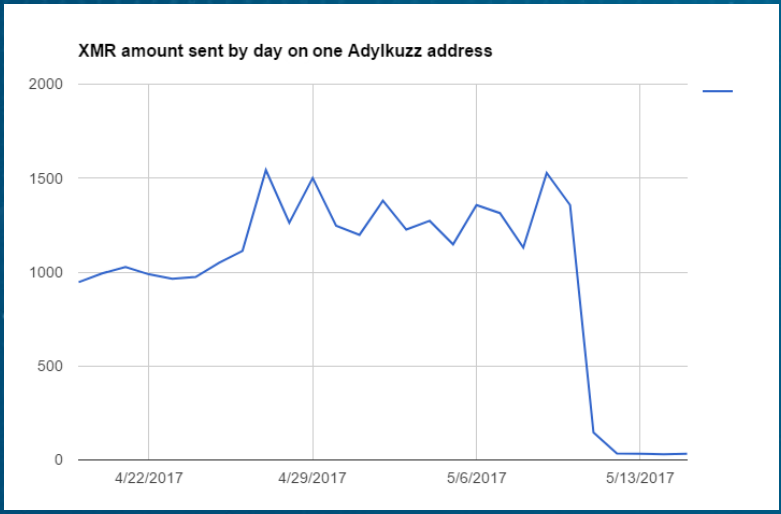
What about the move to crypto-mining and crypto-jacking?

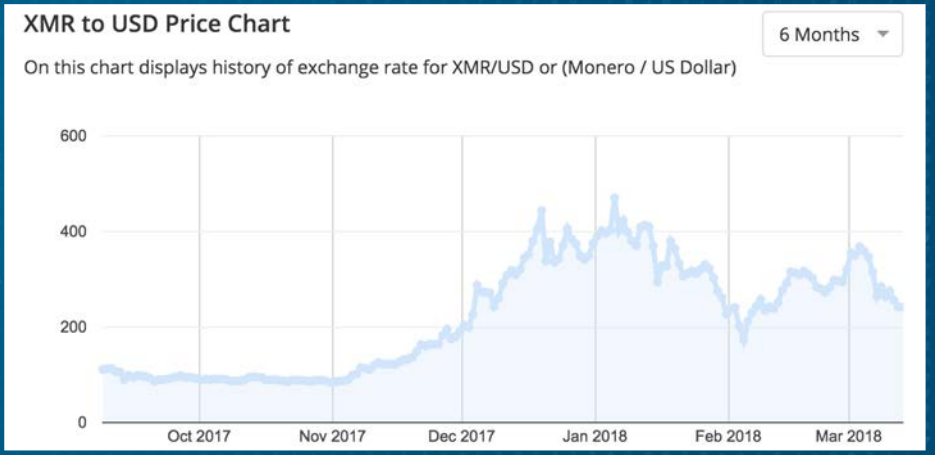
Crypto-mining Malware Started Earlier than WannaCry

- On April 24th, just before WannaCry's release on May 12th, a new malware sample called "Adylkuzz" began spreading using EternalBlue.
- Adylkuzz mined the crypto-currency Monero, whose value continues to climb.
- Adylkuzz shares code with other Lazarus tools and thus may be North Korean.
  - Believed to be the work of Bluenoroff, a Lazarus Group branch that pursues funds for Lazarus activities.
- WannaCry was blocked from infecting some machines, as Adylkuzz deactivates SMB and thus cuts off their shared infection vector.

Adylkuzz's Financial Take

- One Adylkuzz mining address earned between 1,000 and 1,500 XMR per day for roughly 20 days in late April and early May.
- At today's rates, that places the value at between $200k and $300k.





InGuardians™

Server-based Smominru Makes Millions of Dollars

- In May 2017, Smominru Monero mining botnet showed up, using EternalBlue to infect Windows hosts.
- It has made roughly $3 million for its owners.
- Smominru was twice the size of Adylkuzz, with over 525,000 hosts.
- On December 17th, researchers found that it was now targeting SQL servers, both Microsoft SQL Server and MySQL on Linux
- Defies shutdown attempts – Proofpoint's first shutdown cut off one mining account, but the botnet switched to another.

Crypto-mining Moves to the Forefront in the Fall of 2017

- Coinhive announced in mid September that it could mine the Monero cryptocurrency in browsers, providing the bulk of the revenue to anyone hosting its JavaScript library.
- Monero rose in value quickly from around $150 to a December and January peak above $400.

Crypto-jacking in Browsers Escalated Quickly

- Coinhive announced its service on September 14th
- By September 23rd, it was rapidly being integrated into malware.
  - "SafeBrowse" Chrome extension ran mining whenever the browser was active.
  - Attackers registered typo-squatting domains, hosting the Coinhive library.
  - Compromised WordPress sites would include the Coinhive library.
- By mid November, it was estimated that 30,000 sites were running Coinhive's crypto-mining JavaScript code.
- About one month ago, attackers hacked BrowseAloud, a library used by many other companies to add voice assistance to their sites.

Coinhive has Competition

- Coinhive, which gives 70% of the return to site owners, got competition:
- CoinHave gives 80%, with lower minimum payments

and

- Crypto-Loot gives 88%.

Last Month: Crypto-Mining Malware on ICS Servers

- On February 12, a European water utility was discovered to have crypto-mining malware on its servers.
- Luckily, this didn't cause outages or other problems.

Last Week: DoFoil Infects 500k Hosts in One Day

- Microsoft's Windows Defender Research team detected DoFoil on 500,000 hosts in Russia, Ukraine and Turkey, before shutting it down.
- Their first detection occurred in the morning, with 80k hosts.
- Twelve hours later, the botnet was up to 400k hosts.
- By the end of the day, the botnet had reached 500k hosts.
- There were more hosts – Microsoft could only see those running Defender.
- This malware mined Electroneum.
- Caught by behavioral detection via Windows Defender.

This Week: ReddisWannaMine

- March 10: Coinminer Campaigns Target Redis, and Windows Servers
- Worm scans to find vulnerable Redis Linux servers and propagates to them, adding crypto-mining.
- Worm also infects Windows machines with EternalBlue, adding crypto-mining to those as well.

This Week: Apache Solr

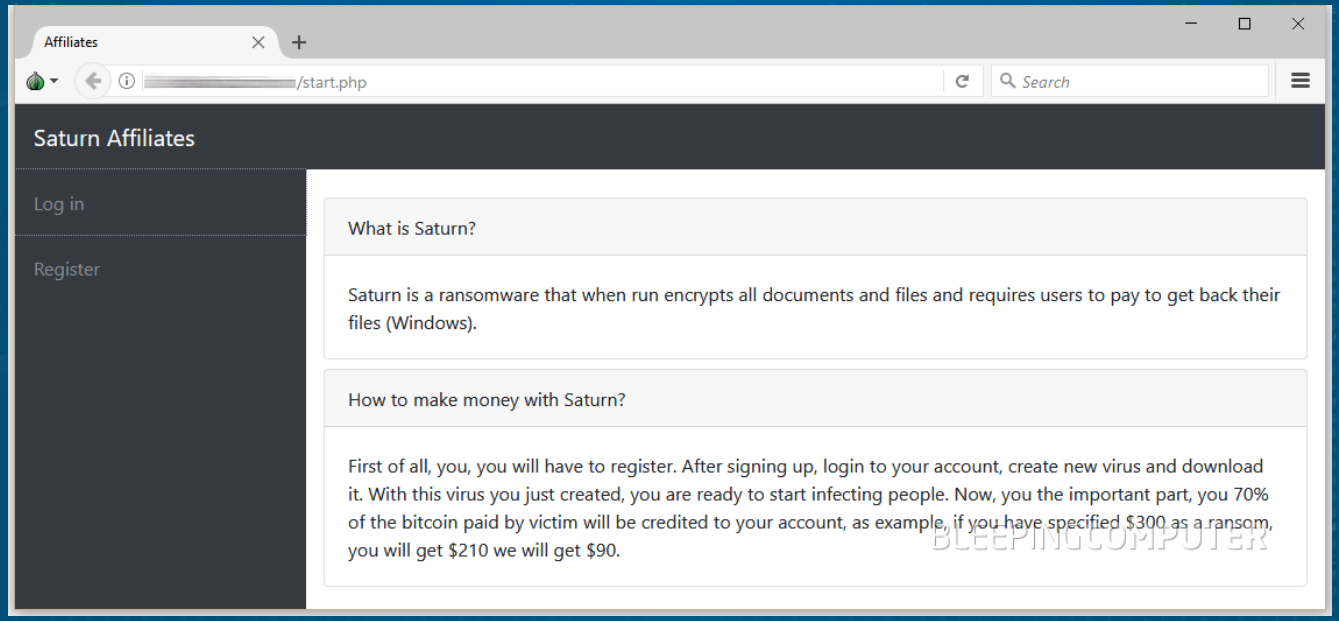
- At the same time that Imperva found the ReddisWannaMine worm, the SANS Internet Storm Center found a worm exploiting Apache Solr to deploy crypto-mining malware.
- One difficulty: Solr is packaged as part of products that you might not realize.
  - Libraries and third party components make patching more difficult than we think.
- Targeting servers gets much higher hash rates (financial return), because the computational resources are more plentiful and stable.

Crypto-Jacking Displacing Ransomware?

- Ransomware feels so much like yesterday's news, as more groups seem to be moving to crypto-jacking.
- But ransomware isn't going away any time soon.
- Colorado's Department of Transportation was crippled three weeks ago.
- It was hit by the same SamSam ransomware infection that caused problems at hospitals, city councils and ICS firms in January.
- Ransomware has hit Android phones, though so has crypto-jacking.
- Tor web proxies have been found stealing ransoms
- Ransomware has even hit robots, in a proof of concept.

Ransomware as a Service (RaaS) Offerings

New Ransomware as a Service offerings are still being released this year.



Crypto-Mining Hasn't Displaced Any Cybercrime

- We still have banking trojans stealing banking logins.
  - They've started stealing cryptocurrency wallets, but they still steal credit cards.
- If a criminal business model works, the attackers are still using it.

NotPetya Inspired More Spreaders

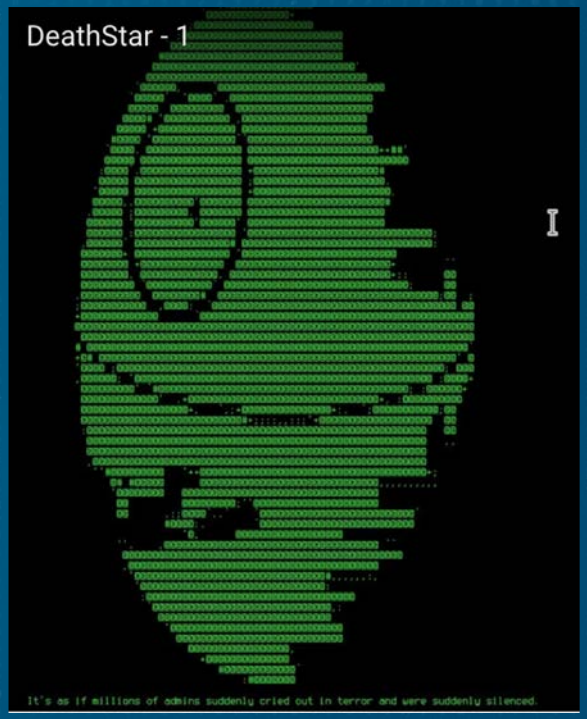
- After NotPetya, the Emotet banking trojan got an unfortunate upgrade.
- Emotet now ships with a LAN-focused spreader.
  - Finds servers on the local network.
  - Attempts 1,000 passwords against any accounts found on each server.
  - Attempts to brute force local Administrator accounts on each server.
- Trickbot version 29 gained a worm module as well, spreading via SMB.
- Researchers are finding other trojan programs, previously spread only by e-mail or website, to now be spreading themselves on LANs.

How Would You Make This Worse?

- What if we added BloodHound to this?
- BloodHound develops graphs of relationships in an Active Directory, to find paths to domain administrators or other users and resources.
- Every defender should now be using this.
- It **will** find unintended relationships or configurations that you'll want to fix.
- We've had this tool for two years.

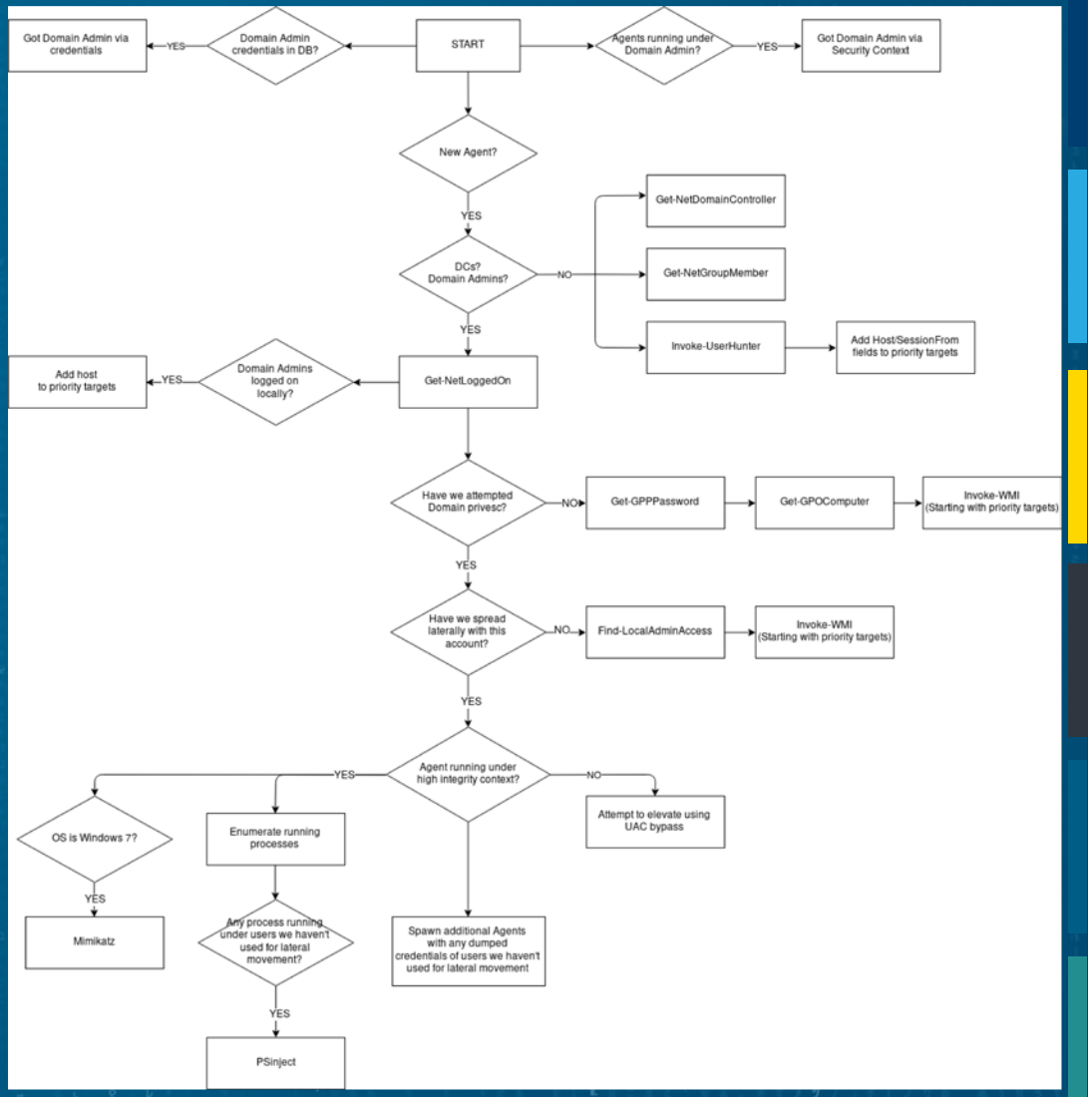
Death Star Takes This Approach

- Death Star isn't using BloodHound, but expanding on the concept.
- Move from a single system to many systems, hunting domain administrators.
- Escalate privilege, move laterally, repeat.
- Death Star does depend on the Empire post-exploitation framework.
- Time permitting, we'll see a Death Star run.



Death Star's Algorithm and Tools

- Get-GPPPassword
  - Gets accounts often admins
- Invoke-WMI
  - Infects a new system via WMI
- Find-LocalAdminAccess
  - Find machines where this has account has access.
- Invoke-UserHunter



The Nightmare: Efficient, DA-Seeking Malware

- This year's worms have implemented spreading, but not full domain-level privilege escalation.
- What if next year's worms integrate/rewrite Death Star and Empire?
- We'll have malware that can gain domain administrative privilege, able to completely control every single A/D-connected endpoint.
- Add BloodHound's speed and it will get to domain administrator (DA) quickly.
- Write a good algorithm and DA will result in quick (exponentially-accelerating) compromise of every single Active Directory-authenticated system.

The Worse Nightmare: Programmatic Plug-in Use of DA

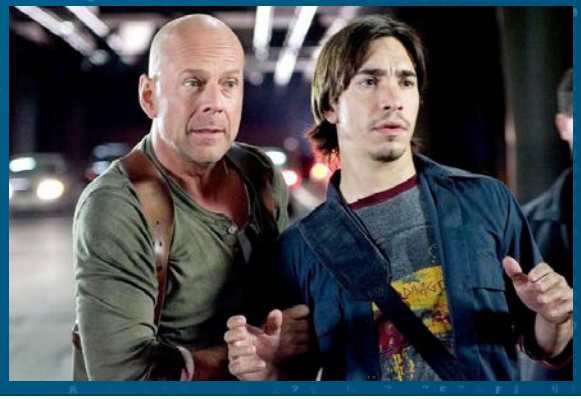
- Pull/modify program-specific data from shares, databases and drives
  - Payment Card Information (PCI): credit cards
  - Banking: ACH and SWIFT banking account numbers and authorizations
  - Personally-identifiable Information (PII): social security numbers, drivers license, …
  - Health information (ePHI): medical conditions, blood type, medication dosages
  - Intellectual Property: source code, relationships and trade secrets
- Now imagine indexing all of that, so you don't have to pull it all.
- Afterwards, deploy cryptocurrency mining and ransomware.

Domain Administrator is the Start, Not the End

- Pull/modify program-specific **access** from shares, databases, and drives
  - Credentials to everything non-A/D authenticated
    - Linux and legacy Unix systems
    - SCADA
    - IoT
    - Mainframes
  - Multi-factor authentication servers
  - AWS and other cloud service API Keys and Root Passwords

And What if the Tools Gave Interactivity

- What if after the tools did all of this, they reported their access to the bad actors, who could begin “operating” the way red teamers and governments do?
  - This attack team fully automated the beginning part of a red team exercise or penetration test.
  - Now, if he can organize all the access he’s being given, things start to play out like the “Fire Sale” in “Live Free or Die Hard!”
  - Yippee Kai Yay, indeed?



What Do We Need to Do?

- What do we need to do to protect ourselves?
- What do we owe each other?

How do we Protect Ourselves?

- NotPetya and other LAN spreaders looked like a very low-end penetration test, by spreading laterally with common penetration test tools.
- The defenses recommended in penetration test reports would beat these tools' lateral movement, as well as that of the two nightmares.
- The only new defense emphasis that NotPetya brought to the table were:
  - Backups
  - Stockpiling Bitcoin for ransoms

Best Practice Protections: the Easy Steps

- Patch systems as if you're in a race. You are.
- Block inbound and outbound SMB ports 135-139 and 445, RDP, SSH, telnet.
- Use separate accounts for:
  - Normal user activities (web browsing, Microsoft Office, e-mail, …)
  - Administering servers or workstations
  - Modifying the domain itself
- Do not allow **any** end users to be local administrator on their systems.
- Run BloodHound against your Active Directory often.

Best Practice Protections: the Harder Steps (1 of 2)

- Assume that you have a compromised computer on your network. You do.
- Prevent servers from making outbound connections to the Internet.
  - Watch your egress logs.
- Apply network segmentation.
  - One compromised system shouldn't be able to get to every other system.
  - Finance shouldn't be able to reach developer machines and vice versa.
- Put workstations on private VLAN's.

Best Practice Protections: the Harder Steps (2 of 2)

- Harden systems with best practices guides from vendors or CIS.
- Build and maintain an inventory of applications and dependencies

What Do We Owe Each Other?

- Strong egress firewalls
- Patching practices to protect the Internet from our machines
- SPF, DKIM, DMARC
- Communication – form relationships with others in the industry and area

Discuss

- What would you add to my nightmare scenarios?
- Why isn't your network segmented?
  - On our red team and penetration test engagements, we find under 5% of networks have any kind of segmentation. When we find it, it works.
- How much have recent malware (ransomware and crypto-mining particularly) influenced your organization's willingness to put time into defenses?
- What other defenses do you have for ransomware, worms and bad actors?
- How interesting is it that economic factors have made worms less common?

A Death Star Run: Overall (0/4)

```
[*] Powering up the Death Star
[*] Polling for agents
[+] New Agent => Name: STFCD8R7 IP: 192.168.10.20 HostName: WIN10 UserName: LAB\yomama HighIntegrity: 0
[*] Agent: STFCD8R7 => Starting recon
[+] Agent: STFCD8R7 => Found 2 members for the '"Domain Admins"' group: ['LAB\\g0d', 'LAB\\Administrator']
[+] Agent: STFCD8R7 => Found 2 Domain Controllers: ['DC1.lab.local', 'DC2.lab.local']
[+] Agent: STFCD8R7 => Found 4 active admin sessions: ['DC1.lab.local', 'DC1.lab.local', 'DC1.lab.local', 'DC2.lab.local']
[+] Agent: STFCD8R7 => Found 1 users logged into localhost: ['LAB\\yomama']
[*] Agent: STFCD8R7 => Starting lateral movement
[*] Agent: STFCD8R7 => Attempting to elevate using bypassuac_eventvwr
[+] Agent: STFCD8R7 => Current security context has admin access to 1 hosts
[+] Agent: STFCD8R7 => Spread laterally using current security context to WIN7OMFGTHISLON.lab.local
[+] New Agent => Name: 7KCLE9XM IP: 192.168.10.25 HostName: WIN7OMFGTHISLON UserName: LAB\yomama HighIntegrity: 1
[+] Agent: 7KCLE9XM => Found 1 users logged into localhost: ['LAB\\yomama5']
[+] Agent: 7KCLE9XM => Enumerated 1 processes
[*] Agent: 7KCLE9XM => Found process 2028 running under LAB\yomama5
[*] Agent: 7KCLE9XM => PSInjecting into process 2028
[+] New Agent => Name: PAT87XLM IP: 192.168.10.25 HostName: WIN7OMFGTHISLON UserName: LAB\yomama5 HighIntegrity: 0
[+] Agent: 7KCLE9XM => Executed Mimikatz
[+] Agent: PAT87XLM => Found 1 users logged into localhost: ['LAB\\yomama5']
[*] Agent: PAT87XLM => Starting lateral movement
[+] Agent: PAT87XLM => Current security context has admin access to 1 hosts
[+] Agent: PAT87XLM => Spread laterally using current security context to WIN7.lab.local
[+] New Agent => Name: S4TK136D IP: 192.168.10.21 HostName: WIN7 UserName: LAB\yomama5 HighIntegrity: 1
[+] Agent: S4TK136D => Found 2 users logged into localhost: ['LAB\\g0d', 'LAB\\yomama4']
[+] Agent: S4TK136D => Found Domain Admin logged in: LAB\g0d
[+] Agent: S4TK136D => Enumerated 1 processes
[*] Agent: S4TK136D => Found process 1524 running under LAB\yomama4
[*] Agent: S4TK136D => PSInjecting into process 1524
[+] New Agent => Name: ADUXGMHZ IP: 192.168.10.21 HostName: WIN7 UserName: LAB\yomama4 HighIntegrity: 0
[+] Agent: S4TK136D => Executed Mimikatz


[+] Got Domain Admin via credentials! => Username: LAB\g0d Password: P@ssw0rd
```

A Death Star Run (1/4)

```
[*] Powering up the Death Star
[*] Polling for agents
[+] New Agent => Name: STFCD8R7 IP: 192.168.10.20 HostName: WIN10 UserName: LAB\yomama HighIn
[*] Agent: STFCD8R7 => Starting recon
[+] Agent: STFCD8R7 => Found 2 members for the '"Domain Admins"' group: ['LAB\\g0d', 'LAB\\Adm
[+] Agent: STFCD8R7 => Found 2 Domain Controllers: ['DC1.lab.local', 'DC2.lab.local']
[+] Agent: STFCD8R7 => Found 4 active admin sessions: ['DC1.lab.local', 'DC1.lab.local', 'DC1
[+] Agent: STFCD8R7 => Found 1 users logged into localhost: ['LAB\\yomama']
```

- First agent starts on system WIN10 with user yomama
- Finds the domain admins group, containing g0d and Administrator
- Finds the domain controllers: DC1 and DC2
- Finds active admin sessions on domain controllers
- Finds 1 user logged into this system

A Death Star Run (2/4)

- Elevates access to SYSTEM or Administrator using an Event Viewer privesc
- Finds a host where yomama is local admin (WIN7OMFGTHISLON)
- Starts agent on it, finds a new user logged in here, called yomama5
- Injects into yomama5's process
- Starts a new agent on this host, using yomama5's context

A Death Star Run (3/4)

```
[+] Agent: 7KCLE9XM => Executed Mimikatz
[+] Agent: PAT87XLM => Found 1 users logged into localhost: ['LAB\\yomama5']
[*] Agent: PAT87XLM => Starting lateral movement
[+] Agent: PAT87XLM => Current security context has admin access to 1 hosts
[+] Agent: PAT87XLM => Spread laterally using current security context to WIN7.lab.local
[+] New Agent => Name: S4TK136D IP: 192.168.10.21 HostName: WIN7 UserName: LAB\yomama5 HighInteg
[+] Agent: S4TK136D => Found 2 users logged into localhost: ['LAB\\g0d', 'LAB\\yomama4']
[+] Agent: S4TK136D => Found Domain Admin logged in: LAB\g0d
```

- Runs mimikatz, gaining yomama5's password
- Determines that yomama5 has administrative access to WIN7
- Pivots to WIN7
- Starts an agent on WIN7
- Finds that WIN7 has the domain administrator g0d logged in

A Death Star Run (4/4)

```
[+] Agent: S4TK136D => Enumerated 1 processes
[+] Agent: S4TK136D => Found process 1524 running under LAB\yomama4
[+] Agent: S4TK136D => PSInjecting into process 1524
[+] New Agent => Name: ADUXGMHZ IP: 192.168.10.21 HostName: WIN7 UserName: LAB\yomama4 HighInte
[+] Agent: S4TK136D => Executed Mimikatz


[+] Got Domain Admin via credentials! => Username: LAB\g0d Password: P@ssw0rd
```

- Injects into yomama 4's process
- Executes Mimikatz
- Gains domain administrator credentials for g0d (password is P@ssw0rd)

Jay Beale is a Linux security expert who has created several defensive security tools, including Bastille Linux/UNIX and the CIS Linux Scoring Tool, both of which were used widely throughout industry and government. He has served as an invited speaker at many industry and government conferences, a columnist for Information Security Magazine, SecurityPortal and SecurityFocus, and a contributor to nine books, including those in his Open Source Security Series and the “Stealing the Network” series. He has led training classes on Linux Hardening and other topics at Black Hat, CanSecWest, RSA, and IDG conferences, as well as in private corporate training, since 2000. Jay is a co-founder, Chief Operating Officer and CTO of the information security consulting company InGuardians.

InGuardians is a leading information security consultancy with offices in Seattle, Boston, Chicago, Dallas, Atlanta and Washington, DC.

INGUARDIANS™