Learn to Detect and Defend Against Supply Chain Attacks Before They Compromise Your Network

Roger A. Grimes
Data-Driven Security Evangelist
rogerg@knowbe4.com

Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

e: rogerg@knowbe4.com
Twitter: @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/

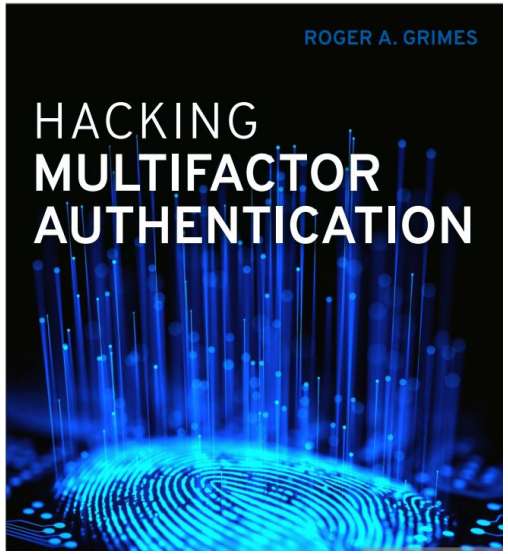
About Roger

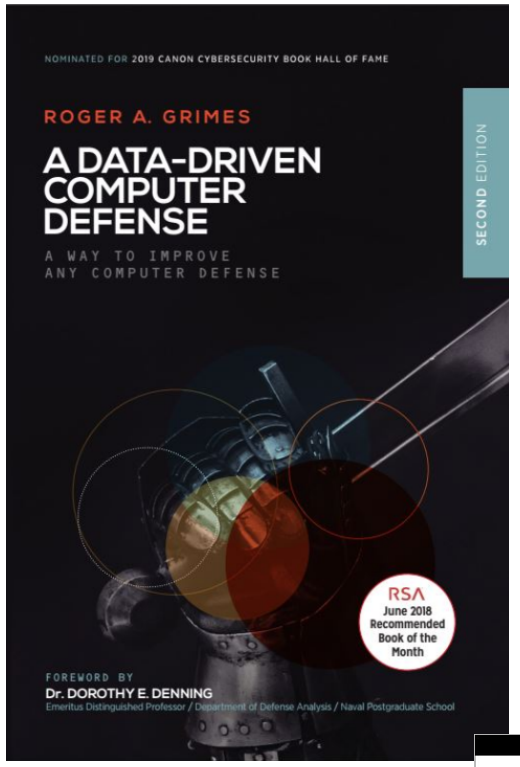
- 30 years plus in computer security, 20 years pen testing
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 12 books and over 1,100 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

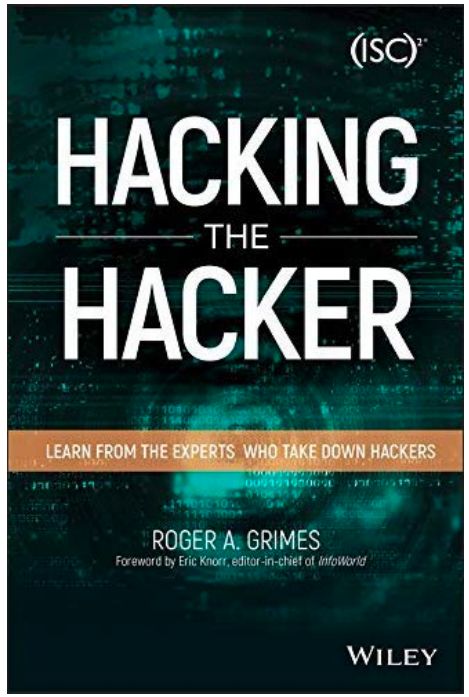
Certification exams passed include:

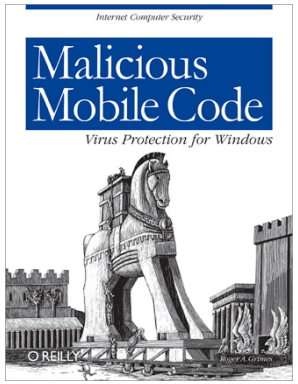
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

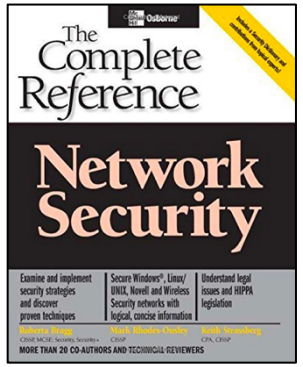
Roger's Books

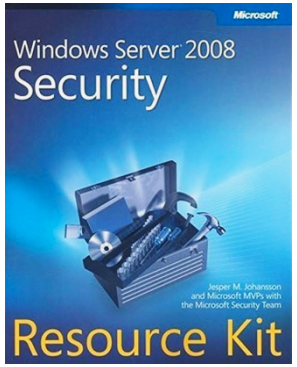


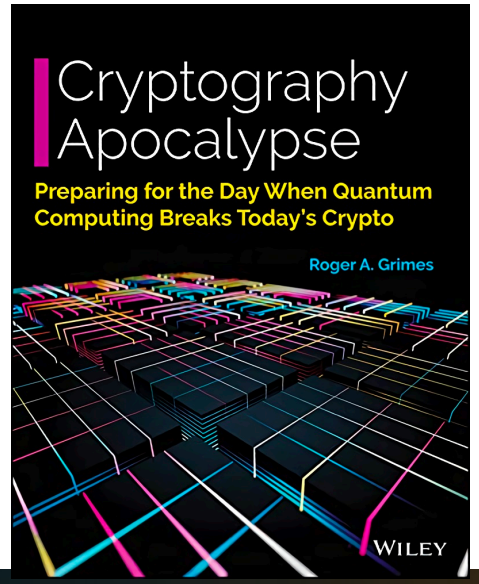


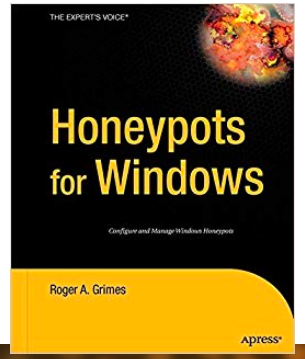


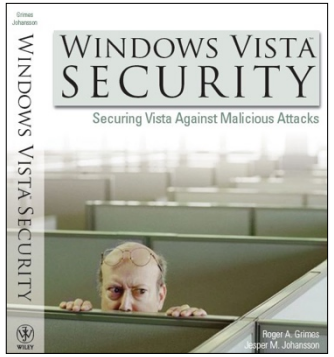


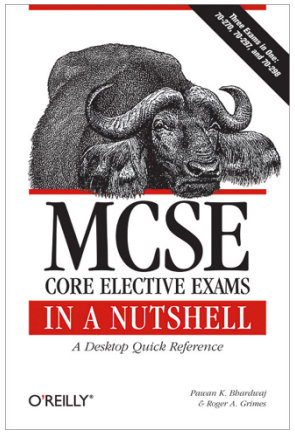












About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- Winner of numerous industry awards

Agenda

- Example Supply Chain Attacks
- Why They Are So Hard to Prevent and Detect
- How to Detect and Stop Them

Supply Side Attacks

Definition

- ***Supply side attacks*** **are exploited vulnerabilities which occurred to or at an upstream trusted entity that ends up impacting a downstream reliant trusting party**
  - Vendor, partner, supplier, hardware, software, site, service, etc.
- Not at all rare
- Been happening for decades
- Just getting far worse lately

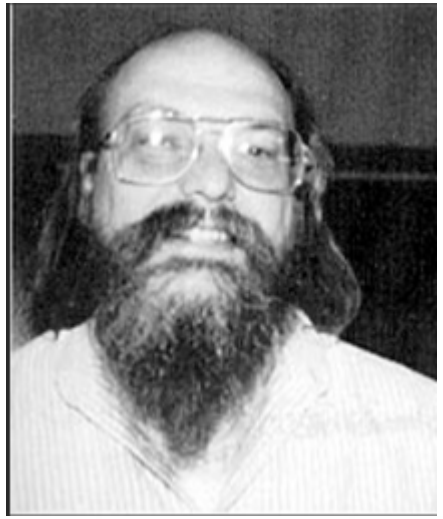
Supply Side Attacks

Same Ole Same Ole

- Maybe you heard about the 2019/2020 '**Solarwinds supply chain attack**' where a nation-state broke into a trust software company and corrupted their compiling process to insert a trojan horse program?

- Who could have ever imagined such a devious attack?

Supply Side Attacks



History

- **Ken Thompson** – father of Unix, UTF-8, multiple prog lang
- **1983** lecture - Turing Award lecture “Reflections on Trust”
- https://dl.acm.org/doi/pdf/10.1145/358198.358210

TURING AWARD LECTURE

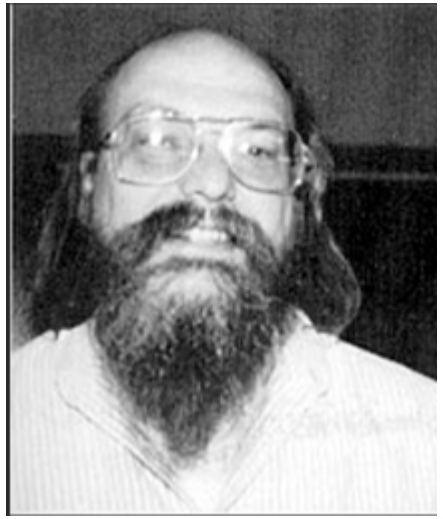
Reflections on Trusting Trust

To what extent should one trust a statement that a program is free of Trojan horses?

MORAL

The moral is obvious. You can’t trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code. In demonstrating the possibility of this kind of attack, I picked on the C compiler. I could have picked on any program-handling program such as an assembler, a loader, or even hardware microcode. As the level of program gets lower, these bugs will be harder and harder to detect. A well-installed microcode bug will be almost impossible to detect.

Supply Side Attacks



History

- **Ken Thompson** – father of Unix, UTF-8, multiple prog lang
- **1983** lecture - Turing Award lecture "Reflections on Trust"
- https://dl.acm.org/doi/pdf/10.1145/358198.358210

TURING AWARD LECTURE

Reflections on Trusting Trus

To what extent should one trust a statement that a program is free of T horses? Perhaps it is more important to trust the people who wrot software.

MORAL

Acknowledgment. I first read of the possibility of such a Trojan horse in an Air Force critique [4] of the security of an early implementation of Multics. I cannot find a more specific reference to this document. I would appreciate it if anyone who can supply this reference would let me know.

crocode. As the level of program gets lower, these bugs will be harder and harder to detect. A well-installed microcode bug will be almost impossible to detect.

Supply Side Attacks

History

- **1974 Multics Security Evaluation: Vulnerability Analysis**, Karger, P.A. and R.R. Schell

ESD-TR-74-193, Vol. II

MULTICS SECURITY EVALUATION:
VULNERABILITY ANALYSIS

Paul A. Karger, 2Lt, USAF
Roger R. Schell, Major, USAF

June 1974

weaknesses. To avoid such a problem and to perpetuate access into the system, the penetrator can install "trap doors" in the system which permit him access, but are virtually undetectable.

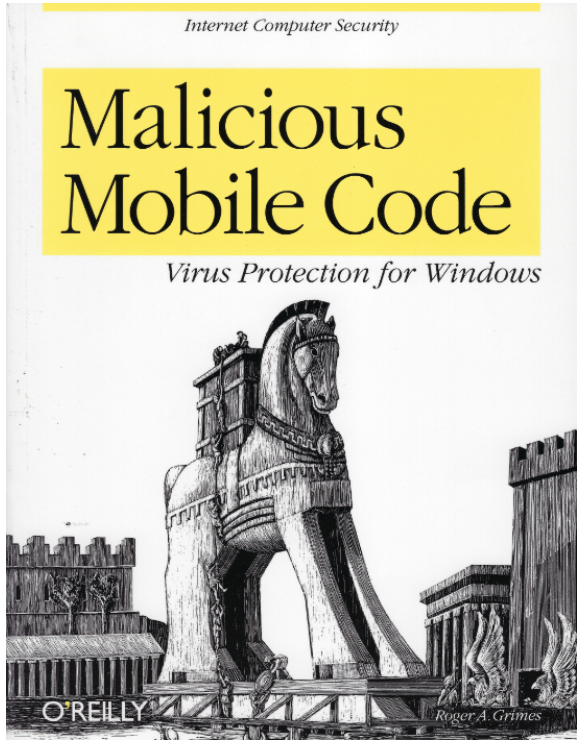
- http://seclab.cs.ucdavis.edu/projects/history/papers/karg74.pdf
  - Section 3.4.5 – Trapdoors, begins on page 50

Supply Side Attacks

History

- **So, yeah, maybe someone already worried about these types of attacks**

1999- cover of my first book



Agenda

- Example Supply Chain Attacks
- Why They Are So Hard to Prevent and Detect
- How to Detect and Stop Them

Supply Side Attacks

History

- Hardware - hard drives, USB keys, iPods, etc., have long come infected with malware from the factory

An iPod arrives, with a virus

CNET News.com's Ina Fried orders a refurbished iPod from Buy.com. It came on time, but with an unwelcome extra file--a Windows virus.

Ina Fried April 30, 2008 9:08 a.m. PT

Last week, I got a sales pitch e-mail from Buy.com touting a recertified 4GB iPod Nano for $99. I lost my iPod Touch last December and one of my older iPods had just given up the ghost, so I decided to go for it.

The iPod came in just a couple of days--but as soon as I unwrapped it and connected it to my Mac at home I got an ominous alert from my usually quiet antivirus software. The iPod, it informed me, contained some virus known as AdobeR.exe

That brand new hard drive could be trying to steal your information

by Evan Dean — 6:44 PM EST, Tue February 16, 2021 AA

Brand new computers found with virus hidden in hard drive

Microsoft employees in China bought 20 new computers from retailers and found malware pre-installed on four.

Chinese Spying Chips Found Hidden On Servers Used By US Companies

October 04, 2018 Mohit Kumar

Supply Side Attacks

History

- Hardware - hard drives, USB keys, iPods, etc., have long come infected with malware from the factory

The NSA's TAO hardware backdoors

Never let it be said that the NSA doesn't have some clever tricks up its sleeve. Recent revelations about its TAO (Tailored Access Operations) program show that one of the NSA's tricks involves intercepting hardware slated for delivery overseas, adding backdoors to the device's firmware, and sending the bugged hardware on its merry way. Aside from network gear, the NSA also apparently planted surveillance software in the firmware for various PCs and even in PC peripherals like hard drives.

Supply Side Attacks

History

- Open source software is constantly compromised

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAM

BIZ & IT —

Questions abound as malicious phpMyAdmin backdoor found on SourceForge site

Secret code added to the package gives attackers the ability to hijack servers.

DAN GOODIN - 9/25/2012, 2:05 PM

Backdoor in e107 CMS version 0.7.17

[Posted January 25, 2010 by jake]

Back door in ProFTPD FTP server

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE S

POISONING THE WELL —

Widely used open source software

bitcoin-stealing backdoor

pt into event-stream JavaScript library went undetected for weeks.

Joomla Plugin Constructor Backdoor

APRIL 23, 2014 DENIS SINEGUBKO

kernel.org compromised

[Posted August 31, 2011 by corbet]

The main kernel.org page is currently carrying a notice that the site has suffered a security breach. "Earlier this month, a number of servers in the kernel.org infrastructure were

Supply Side Attacks

History

- Commercial “lower-tier” software is constantly compromised

Unmasking “Free” Premium WordPress Plugins

MARCH 26, 2014 DENIS SINEGUBKO

SEOPressor

Retail Price: **$47+**

1. When a webmaster installs this plugin, it immediately (on the first blog page load) sends an email with the blog address to the attacker (**thomasza@gmx.com**).
2. Then the attacker comes to the blog and loads it passing the *?cms=jjoplmh* parameters in the URL.
3. As a result, a new admin user (with the “**wordpress**” name and a known password) is created.
4. The attacker can now log into WordPress with admin permissions and do whatever he wants with the blog, with the whole site (e.g. injecting a backdoor to some theme or plugin, and then using it to upload malicious files to the server), with the server account (all sites that share the same account can be easily compromised now) and even with the whole server.

Supply Side Attacks

Water Hole Attacks

- Basic Method
  - Step 1 - Malicious hacker compromises legitimate code sharing web site or poses as a regular user
  - Step 2 - Compromises someone else's existing code or places new code with backdoor trojan
  - Step 3 - Legitimate, unsuspecting, developers download trojan code and use in their own projects

Supply Side Attacks

Waterhole Attacks

- PHP main code repository compromised to place trojan
  - PHP is the most common web site scripting language on the Internet

{* SECURITY *}

PHP repository moved to GitHub after malicious code inserted under creator Rasmus Lerdorf's name

Backdoor quickly spotted and reverted

Tim Anderson Mon 29 Mar 2021 // 11:46 UTC

"Yesterday (2021-03-28) two malicious commits were pushed to the php-src repo from the names of Rasmus Lerdorf and myself. We don't yet know how exactly this happened, but everything points towards a compromise of the git.php.net server (rather than a compromise of an individual git account)," said PHP maintainer Nikita Popov, who works with the PHP team at JetBrains.

The main code repository for PHP, which powers nearly 80 per cent of the internet, was breached to add malicious code and is now being moved to GitHub as a precaution.

Supply Side Attacks

Waterhole Attacks

- 11/2020-PHP main code repository scanned for malware

Researchers Scan for Supply-Side Threats in Open Source

A recent project to scan the main Python repository's 268,000 packages found only a few potentially malicious programs, but work earlier this year uncovered hundreds of instances of malware.

Attackers Aim at Software Supply Chain with Package Typosquatting

Attackers seed Ruby Gems repository with more than 760 malicious packages using names just a bit different than the standard code libraries.

- https://www.darkreading.com/application-security/researchers-scan-for-supply-side-threats-in-open-source/d/d-id/1339465
- https://www.darkreading.com/application-security/attackers-aim-at-software-supply-chain-with-package-typosquatting/d/d-id/1337611

Supply Side Attacks

Water Hole Attacks

- GitHub Waterhole attacks
  - GitHub is a popular open source/commericial platform used by developers to track, store, and reuse code

Supply chain attack hits 26 open source projects on GitHub

Threat actors conducted an unprecedented supply chain attack by using malware known as Octopus Scanner to create backdoors in open source projects, which were uploaded to GitHub.

By **Arielle Waldman**, News

After investigating the malware, the GitHub's security incident response team uncovered 26 OSS projects that were compromised by the malware and actively serving backdoored code. Additional analysis revealed

ished: **28 May 2020**

Supply Side Attacks

Waterhole Attacks

Just a problem of these clueless open source idiots, right?

Supply Side Attacks

Water Hole Attacks – Real-World Example

- In 2013, Microsoft, Facebook, Twitter, Google, Apple hacked by same waterhole exploit

ATTACKS/BREACHES

2/25/2013
12:01 PM

Microsoft Hacked: Joins Apple, Facebook, Twitter

Microsoft's OS X users compromised by watering-hole attack launched from a third-party iOS development site.

and Twitter. Namely, in what's called a watering-hole attack, whoever launched these attacks first compromised the popular iPhoneDevSDK website, without tipping off the website's administrator, and then used the site to launch drive-by attacks against anyone who visited. The attacks, which targeted a zero-day vulnerability in the Java browser plug-in that's since been patched by Oracle, were obviously quite effective, because they affected OS X systems at Apple, Facebook, Microsoft and Twitter.

https://www.darkreading.com/attacks-and-breaches/microsoft-hacked-joins-apple-facebook-twitter/d/d-id/1108800

Supply Side Attacks

Waterhole Attacks

But once bit, they'd never fall for this same type of attack again, right??…

Supply Side Attacks

Water Hole Attacks – Real-World Whitehat Example

- In **2021**, Apple, Microsoft, etc. hacked by a researcher using a waterhole exploit

Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies

The Story of a Novel Supply Chain Attack

Alex Birsan Feb 9 · 11 min read ★

Results

The success rate was simply astonishing.

was detected inside more than 35 organizations to date, across all three tested programming languages. The vast majority of the affected companies fall into the 1000+ employees category, which most likely reflects the

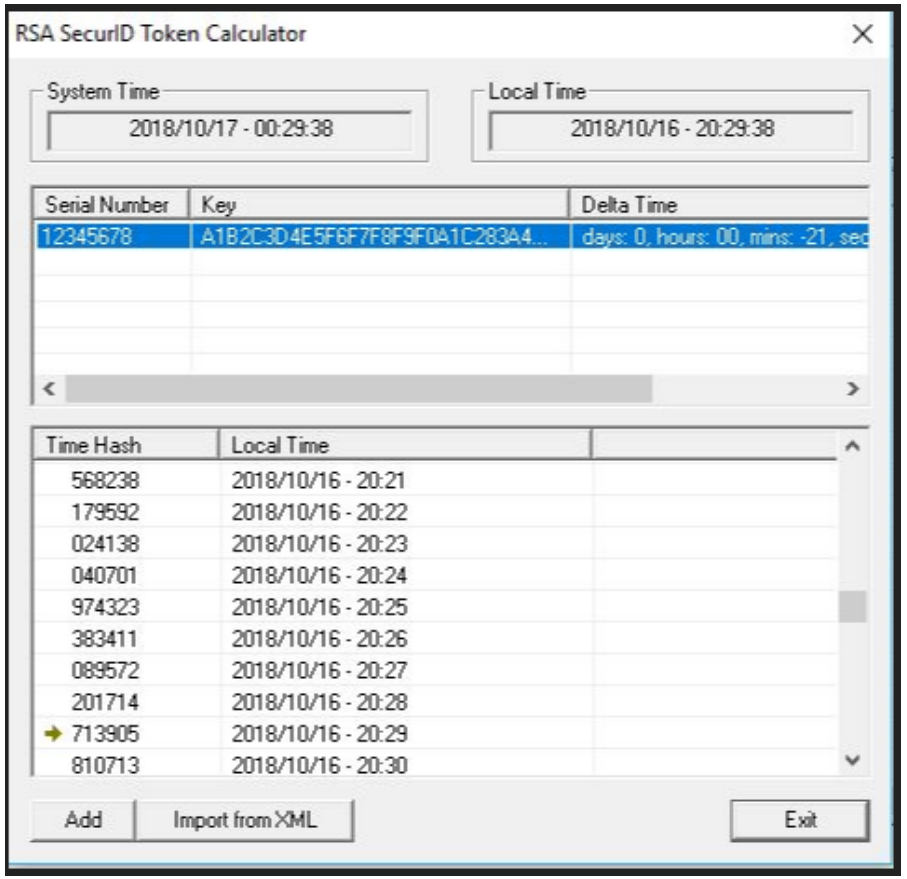
- He learned commonly used GitHub component for accepting Paypal transactions had private dependency names, meant to point to Paypal…but if he created trojan versions with the same name and uploaded, other projects would run the trojan versions instead (known as *package typosquatting*)
- Impacted 35+ co's, including: Shopify, Netflix, Yelp, Uber
- https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

Supply Side Attacks

History

2011 RSA attack

- Hackers broken in and stole RSA's "seed" databases for customer RSA SecurID tokens
- Then broke into customers, including Lockheed Martin
- https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/

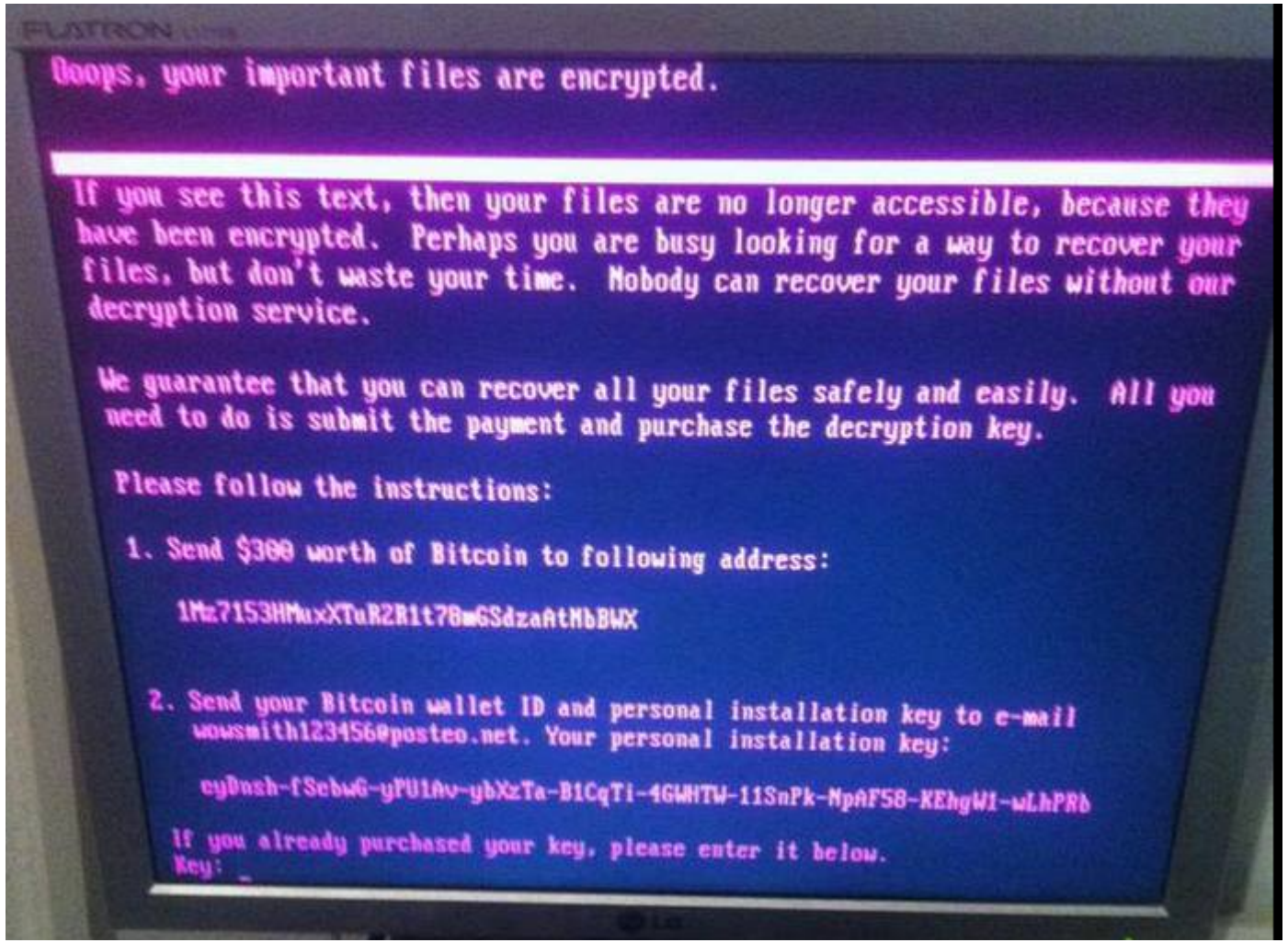


Supply Side Attacks

History

2017 Petya/NotPetya "Ransomware"

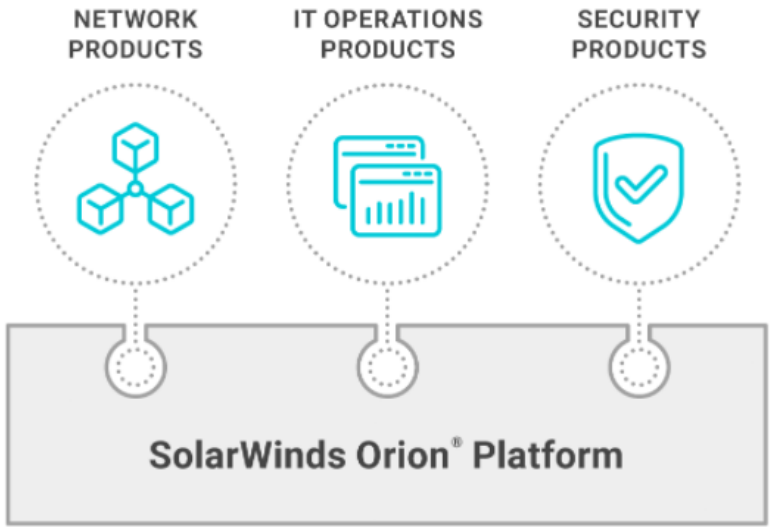
- Basically, cyberwarfare that took out Ukraine
- Placed in accounting software M.E. Doc update servers
  - The "QuickBooks of Ukraine"
- Which was then run by 90% of Ukrainian firms
- 400,000 company infections, 1M overall



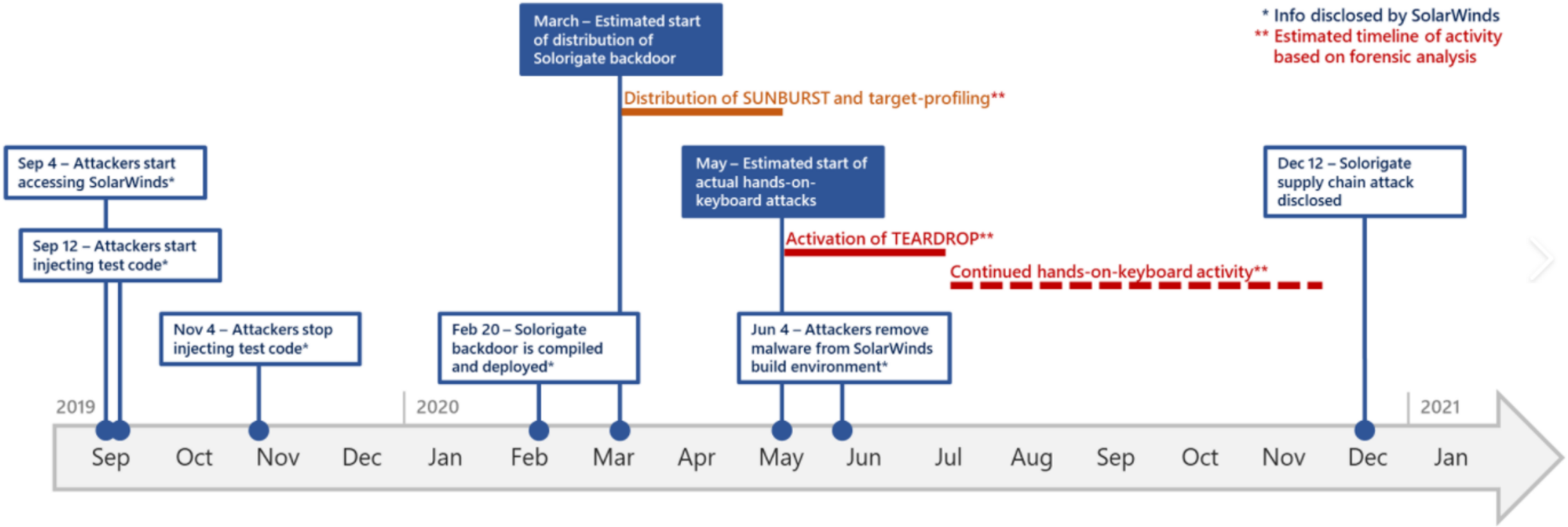
Example Supply Side Attacks

2019-2020 Solarwinds Attack

- APT breaks in to Solarwinds in Sept. 2019
- Modifies software build process of Orion software to include backdoor program
  - SolarWinds.Orion.Core.BusinessLayer.dll
- They tested, then moved to production by March 2020



Example Supply Side Attacks



Taken from: https://securityaffairs.co/wordpress/113681/apt/microsoft-solorigate.html

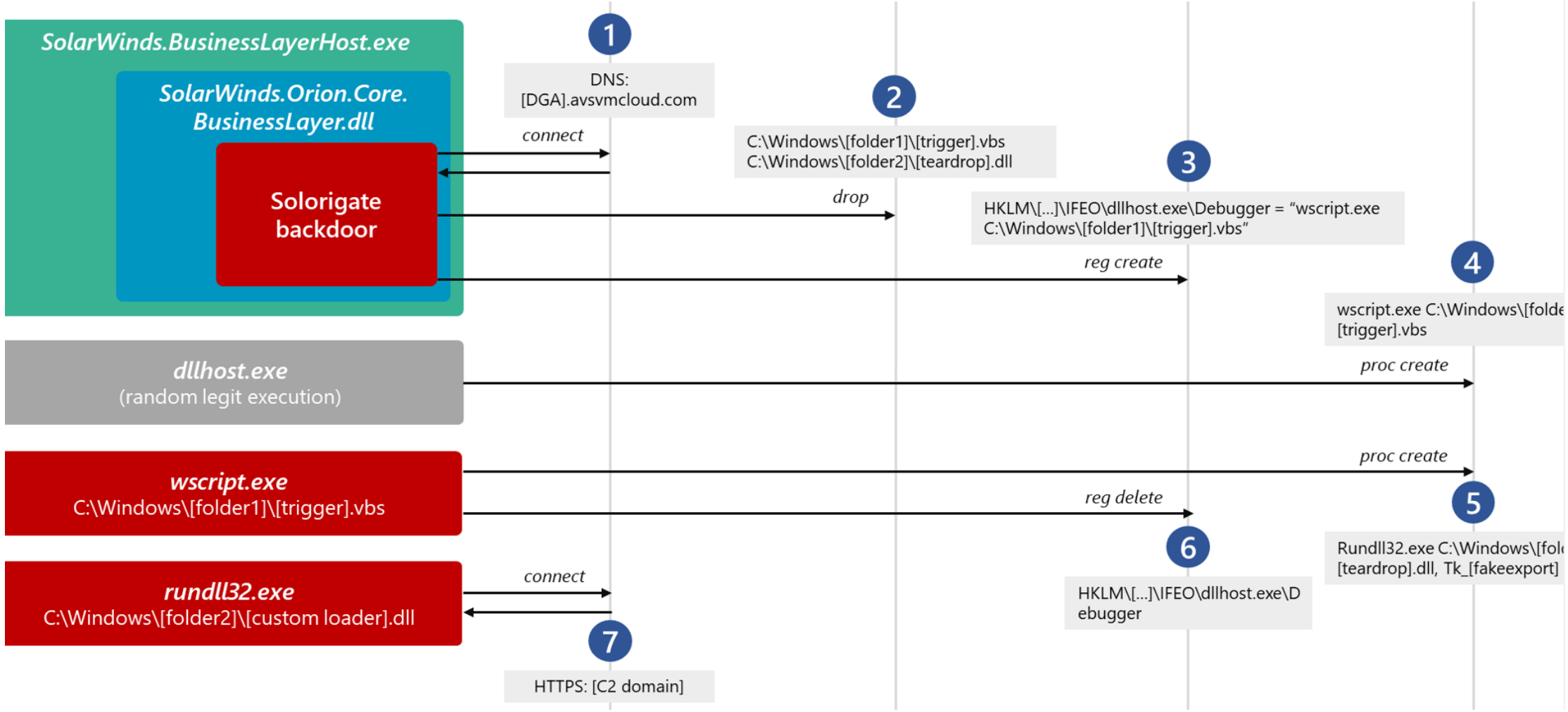
Example Supply Side Attacks

Solarwinds Attack

- From Mar – June 2020, when customers got latest Orion version, trojan built in
  - Attackers remove back door by June
- First publicly reported Dec 2020
- Trojan was digitally signed

- Solarwinds exploited customers included: 425 of the US Fortune 500, the top 10 US telecommunications companies, the top 5 accounting firms, all US military branches, the Pentagon, Dept. of Treasury, Nuclear Regulatory Agency, CDC, Justice Dept, the US State Department, as well as hundreds of universities and colleges

Example Supply Side Attacks



Taken from: https://securityaffairs.co/wordpress/113681/apt/microsoft-solorigate.html

Example Supply Side Attacks

Solarwinds Attack (con't)

- APT actively exploited multiple Microsoft and Vmware 0-day flaws
- Bypassed MFA
- Trojan waited 12-14 days before connecting outbound to C&C servers
- Trojan traffic mimicked legitimate Orion API traffic (but to new domains)
- Used Orion backdoor to compromise top notch US computer security companies including FireEye, Crowdstrike, and Microsoft
- Stole redteam attack tools from FireEye

Agenda

- Example Supply Chain Attacks
- Why They Are So Hard to Prevent and Detect
- How to Detect and Stop Them

Why So Hard to Detect and Prevent?

Summary

- Very unexpected
- Often part of legitimate, signed executables
- Most use TLS to communicate out
- Often used by elite teams (e.g. nation-states)
- False sense of security “Everyone’s using it!”

Agenda

- Example Supply Chain Attacks
- Why They Are So Hard to Prevent and Detect
- How to Detect and Stop Them

Notes

- This coverage is a mile-wide and an inch-deep
- Meant to discuss the various methods anyone can use, but is not meant to be a detailed discussion into anyone technique

Notes

- **Prevention is preferred over detection**

- **Complete perfect protection will never be accomplished until the Internet is made far safer; individual organizations have a far harder time preventing otherwise**

How to Detect and Prevent

Two Distinctly Different Types of Defenders

- Original, “top-level” exploited organization

or

- Downstream victim

- Which is your organization?
  - Both?

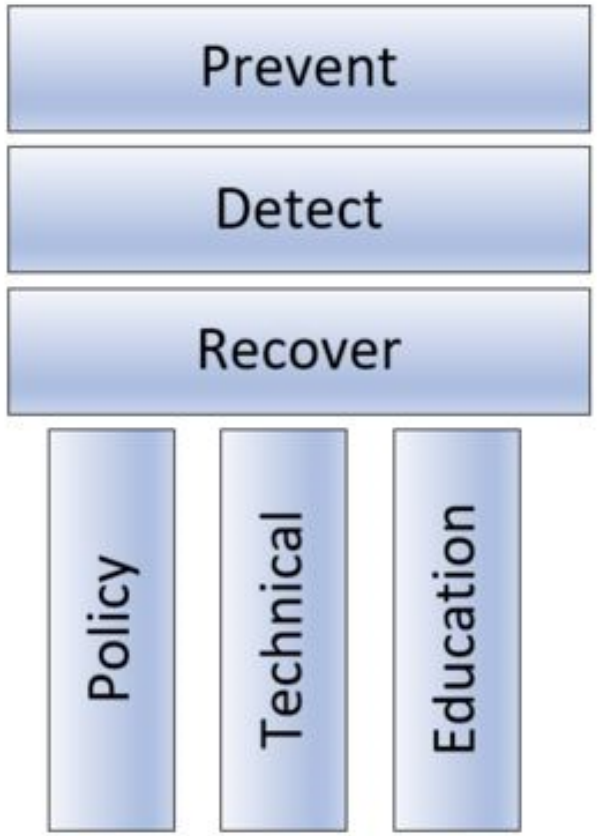
How to Detect and Prevent

Original, Top-Level Victim

- Must stop initial exploitation that allows attackers to get in

3 x 3 Security Control Pillars

For every high-risk threat you want to mitigate, create 3 x 3 controls

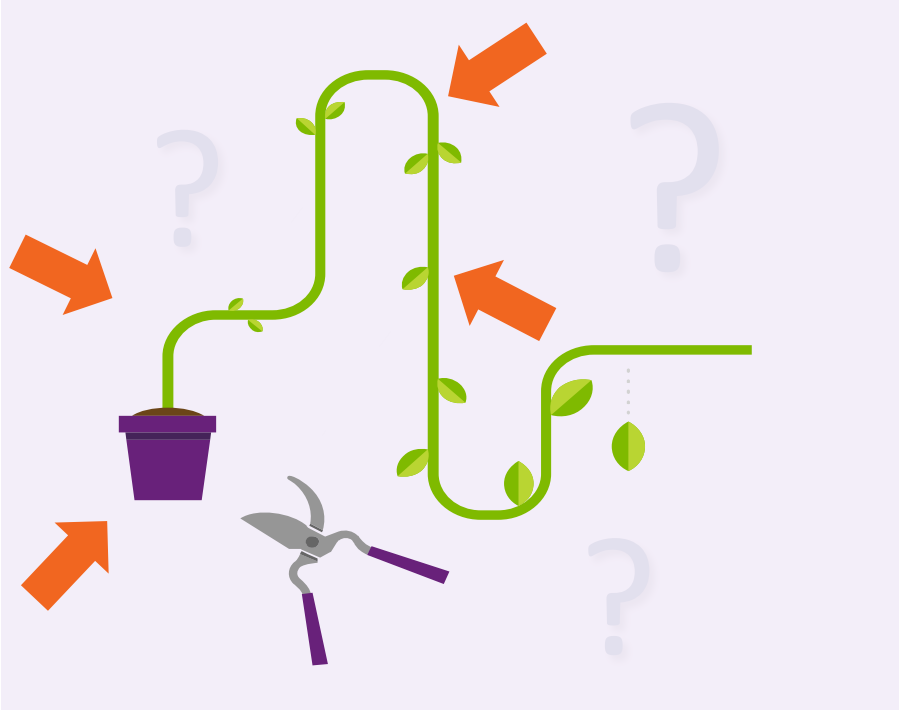


3 x 3 Security Control Pillars - https://www.linkedin.com/pulse/3-x-security-control-pillars-roger-grimes

How Hackers and Malware Break In

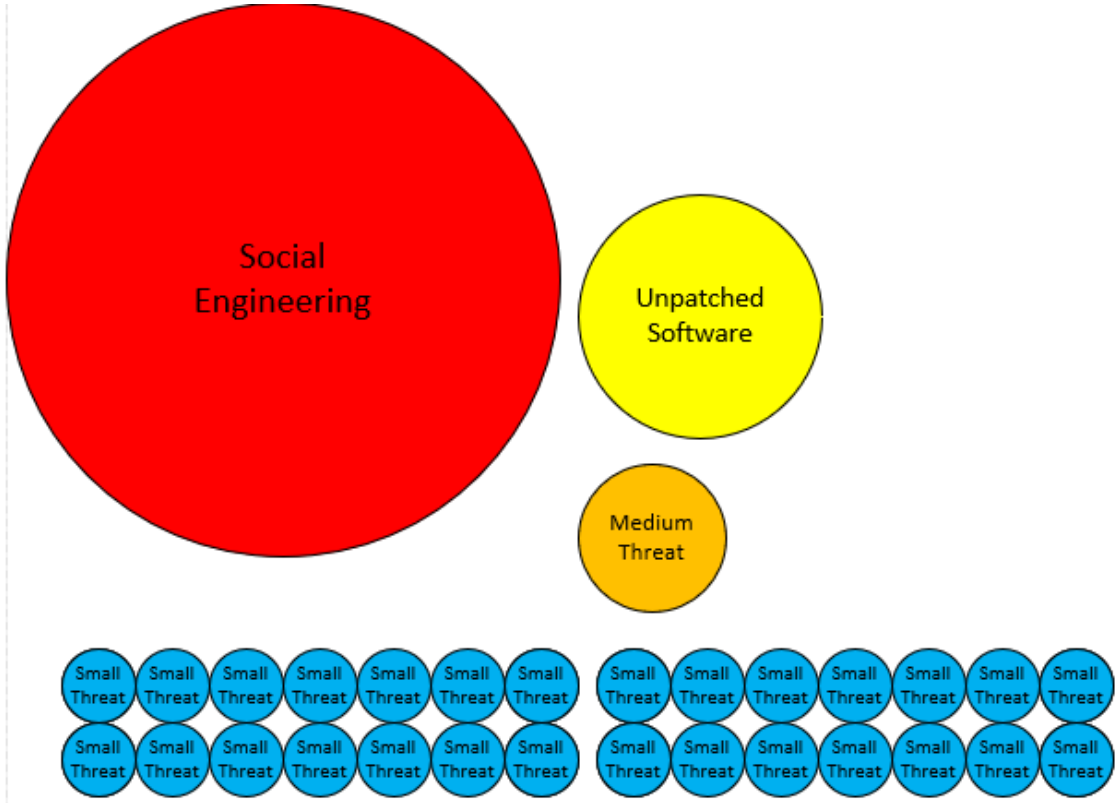
Here Are the Root Exploit Methods:

- Programming Bug
- Social Engineering
- Authentication Attack
- Human Error
- Misconfiguration
- Eavesdropping/MitM
- Data/Network Traffic Malformation
- Insider Attack
- 3rd Party Reliance Issue
- Physical Attack



Biggest Initial Breach Root Causes for Most Companies

- Social Engineering
- Unpatched Software
- But don’t trust me, measure your own risk



Social engineering is responsible for majority of malicious data breaches

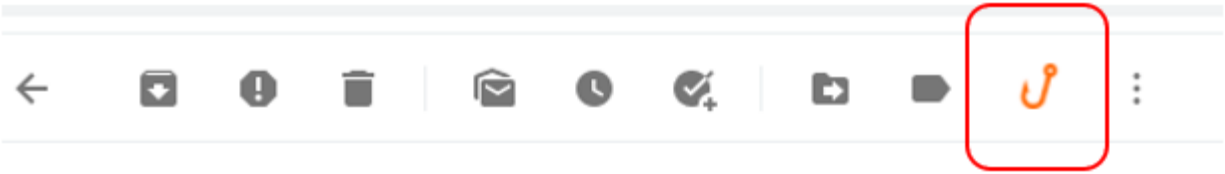
https://blog.knowbe4.com/phishing-remains-the-most-common-form-of-attack
https://info.knowbe4.com/threat-intelligence-to-build-your-data-driven-defense

Best Defenses

Attackers Got In Some Way – Stop Them

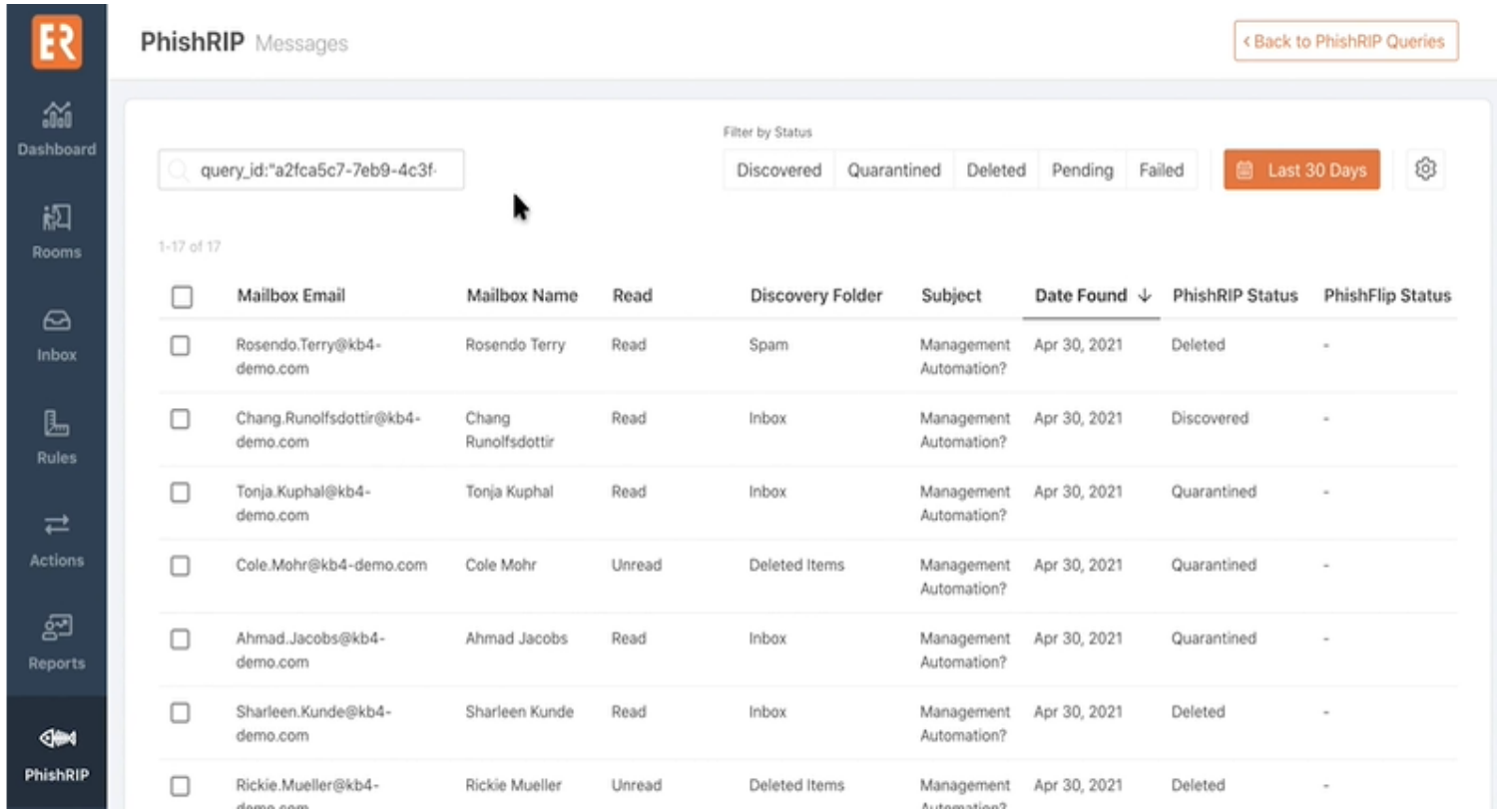
- **Mitigate Social Engineering**
- **Patch Internet-accessible software**
- **Use non-guessable passwords/multifactor authentication (MFA)**
  - Different passwords for every website and service
- **Use Least-Permissive Permissions**
- **Aggressive monitoring, anomaly detection, and alerting**
- **Then follow the stuff I discuss for downstream victims discussed soon**

PhishFlip



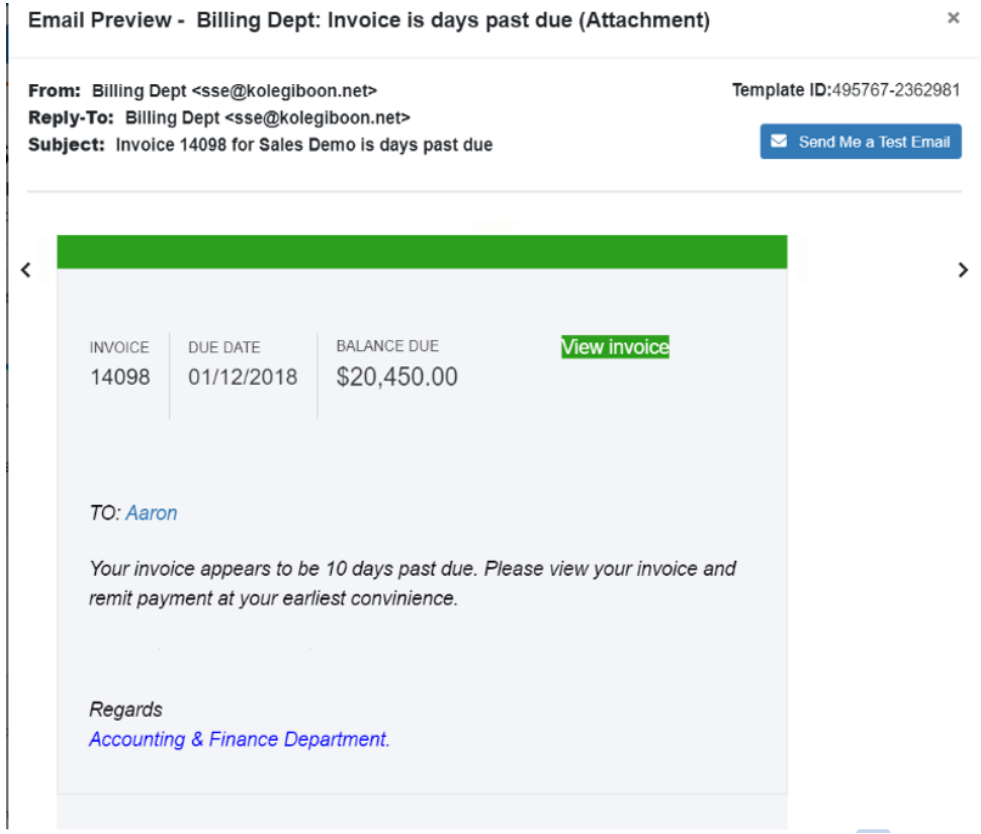
https://blog.knowbe4.com/new-phisher-feature-flip-the-script-on-phishing-emails-with-phishflip

PhishRip



https://blog.knowbe4.com/new-phisher-feature-flip-the-script-on-phishing-emails-with-phishflip

PhishFlip



https://blog.knowbe4.com/new-phisher-feature-flip-the-script-on-phishing-emails-with-phishflip

Best Defenses

For Developers

Secure Code Reuse

- Educate developers about the risk of waterhole attacks
- Implement policies to prevent or minimize external code reuse
  - Always ask, could this borrowed code be used to undermine the security of my/our code?
  - Could we do it ourselves instead?
- Prevent accidental credential leaks in dev code
- Educate all developers in Security Development Lifecycle (SDL) tools and techniques

Best Defenses

For Developers

Secure Source Code Repository

- Use strongly secure source code repository, not accessible on normal network
- Limit inbound pathways to source code repositories
- Strongly monitor inbound connections to source code repositories
- Require strongly secure dev machines (maybe red/green setup)
- Require strong MFA for all devs
- Require multiple reviews for new code check-ins and updates
  - Assume all updates are malicious until otherwise confirmed?
  - Always question unexpected new additions
- Do source code review (human and automate)

How to Detect and Prevent

Downstream Victim Defenses

- Educate all IT staff/+ about supply side attack risks with examples
- Know what software is running on your network

or even better

- Lock your software to only pre-approved software
- Know your network connections
- Alert on anomalous unexplained processes and connections

How to Detect and Prevent

Downstream Victim Defenses

- Know what software is running on your network

or even better

- Lock your software to only pre-approved software
- Most companies don't have a clue as to what is running on all devices
- You probably don't have a clue about what is really running on your own personal devices
- I don't know what is running on my current devices

How to Detect and Prevent

Downstream Victim Defenses

- K
or
- L
- M
- Y
  c
- I

Process Explorer - Sysinternals: www.sysinternals.com [940D38AD-04B4-4\WDAGUtilityAccount] (Administrator)

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
Registry		5,156 K	21,164 K	144			The system canno...
Memory Compression		208 K	19,840 K	1160			The system canno...
KypticRansomware.exe	0.01	10,376 K	20,124 K	5372	Beta Results Mega Pump Rh...	Facebook	58/72
mmc.exe	0.01	134,632 K	181,892 K	1368	Microsoft Management Cons...	Microsoft Corporation	0/73
mmc.exe	0.01	63,604 K	15,680 K	3684	Microsoft Management Cons...	Microsoft Corporation	0/73
WmiPrvSE.exe		2,464 K	8,460 K	7992	WMI Provider Host	Microsoft Corporation	0/72
winlogon.exe		2,612 K	11,840 K	2964	Windows Logon Application	Microsoft Corporation	0/72
WindowsInternal.ComposableSh...		10,680 K	47,296 K	2312	WindowsInternal.Composabl...	Microsoft Corporation	0/72
VmComputeAgent.exe		1,776 K	8,316 K	2284	Hyper-V Guest Compute Ser...	Microsoft Corporation	0/72
taskhostw.exe		11,432 K	23,136 K	3380	Host Process for Windows T...	Microsoft Corporation	0/72
SystemSettingsBroker.exe		5,584 K	23,768 K	996	System Settings Broker	Microsoft Corporation	0/72

How to Detect and Prevent

Downstream Victim Defenses

- Know what software is running on your network

or even better

- Lock your software to only pre-approved software
- Most companies don't have a clue as to what is running
- Use any product that can help you track and alert on new processes
  - Application Control programs
  - Endpoint Detection and Response
  - CrowdStrike, FireEye, Microsoft ATP, etc.
- Research new processes to final resolution

How to Detect and Prevent

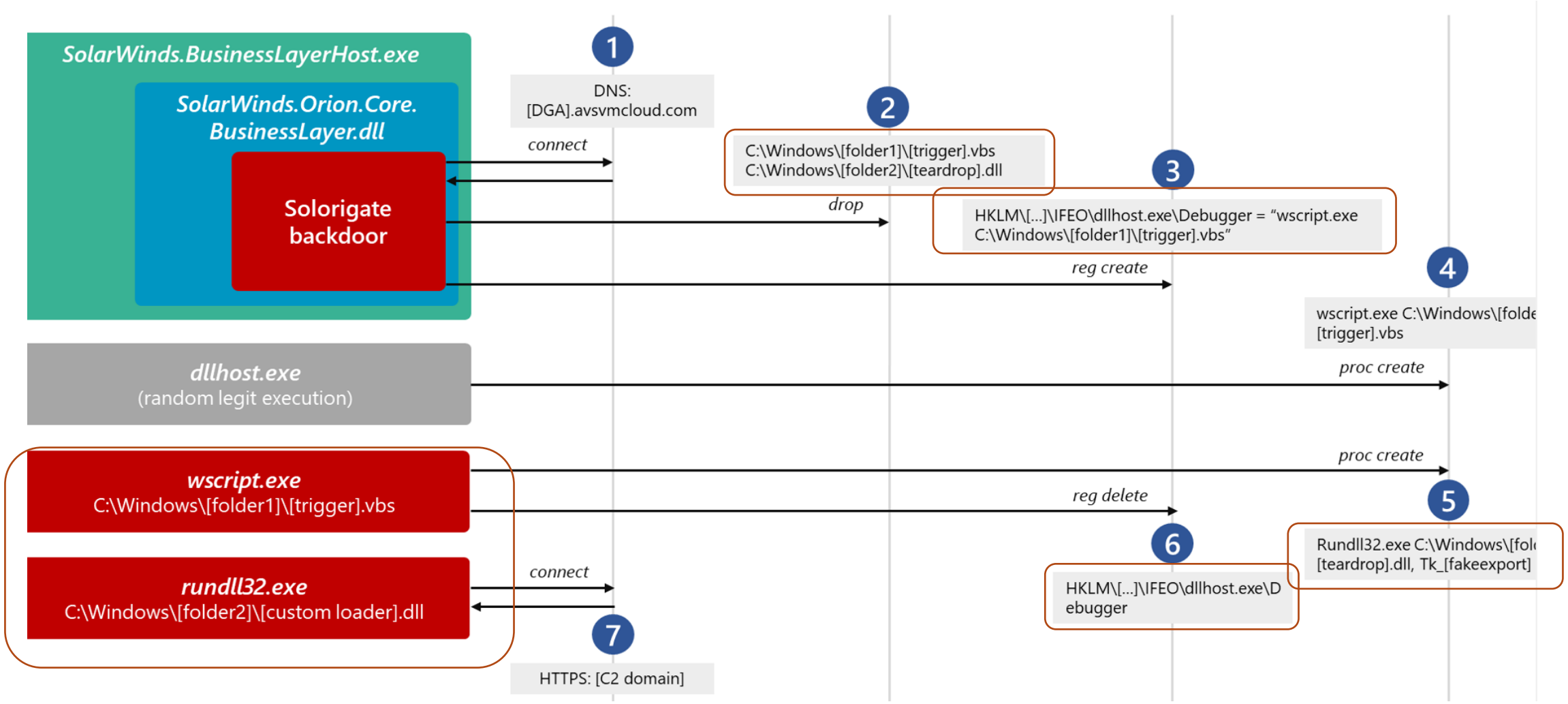
Downstream Victim Defenses

But don't supply side attacks use already existing, approved, software?

- Yes
- But almost always the attackers then upload and use other, non-approved software or scripts and perform non-normal actions
- Perform lateral movement away from initial compromised host

- Initial compromise hard to prevent and detect, but what they do next is not as hard

Solarwinds Attack



Taken from: https://securityaffairs.co/wordpress/113681/apt/microsoft-solorigate.html

How to Detect and Prevent

Other Examples

Alert process tree

New trojan executable

Figure 2. Microsoft Defender ATP alert for credential theft

No rogue executables involved at first, but first time or unexpected use of some executable

Alert process tree

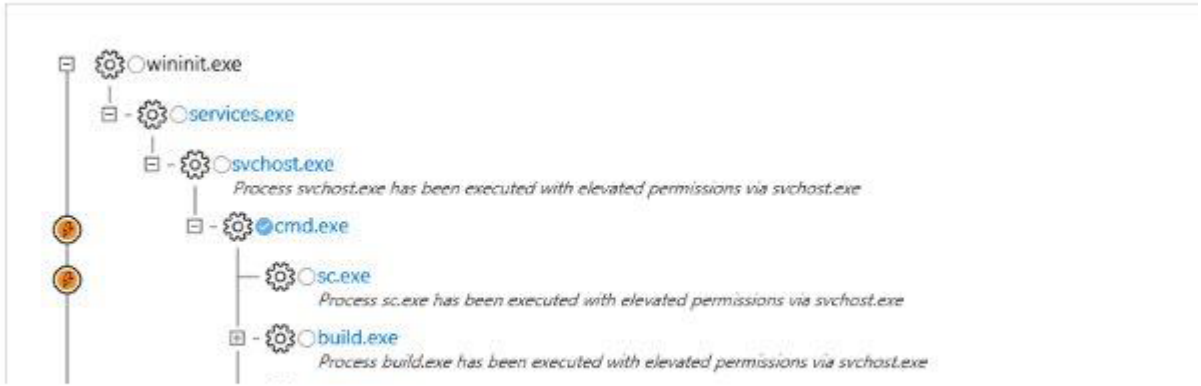


Figure 6. Sample Microsoft Defender ATP alert

From: https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

How to Detect and Prevent

Downstream Victim Defenses

Process Analysis – Unexpected Status Changes

- Explore unexpected/unexplained stopped processes
- Attackers often disable your AV and other defenses
- Conduct “heartbeat” tests, alert on a negative response
- Attackers often disable database engines to copy data
- Attackers often disable backups
- Attackers often enable new malicious tasks or kill existing tasks

How to Detect and Prevent

Downstream Victim Defenses

Process Analysis – Unexpected Changes

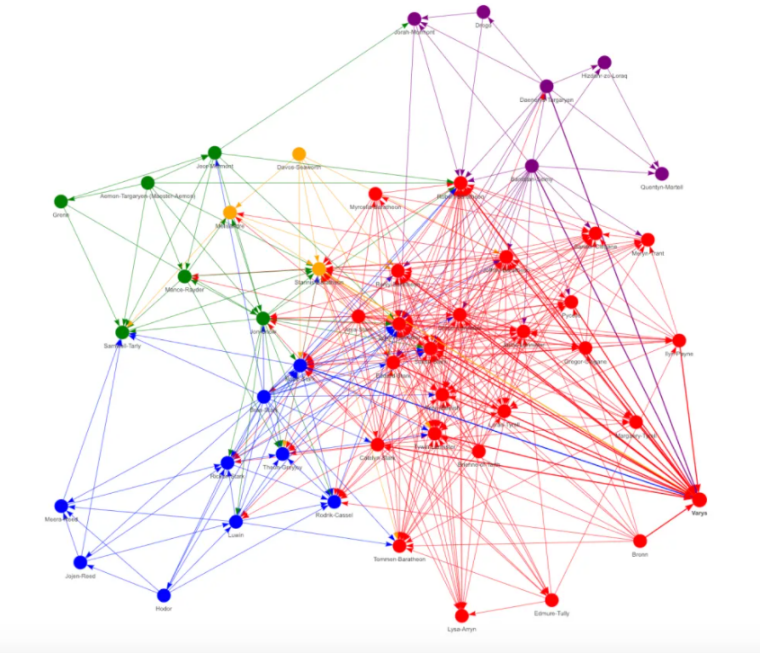
Malware Example - PARINACOTA

```
taskkill  /f /im mysql*
taskkill  /f /im IBM*
taskkill  /f /im bes10*
taskkill  /f /im black*
taskkill  /f /im sql
taskkill  /f /im store.exe
taskkill  /f /im sql*
taskkill  /f /im vee*
taskkill  /f /im postg*
taskkill  /f /im sage*
```

```
net  stop MSSQLServerADHelper100
net  stop MSSQL$ISARS
net  stop MSSQL$MSFW
net  stop SQLAgent$ISARS
net  stop SQLAgent$MSFW
net  stop SQLBrowser
net  stop ReportServer$ISARS
net  stop SQLWriter
net  stop WinDefend
net  stop mr2kserv
net  stop MSExchangeADTopology
net  stop MSExchangeFBA
net  stop MSExchangeIS
net  stop MSExchangeSA
net  stop ShadowProtectSvc
net  stop SPAdminV4
net  stop SPTimerV4
net  stop SPTraceV4
net  stop SPUserCodeV4
net  stop SPWriterV4
net  stop IISADMIN
net  stop QuickBooksDB15
net  stop QuickBooksDB17
net  stop QuickBooksDB18
net  stop QuickBooksDB21
net  stop QuickBooksDB24
```

From: https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

How to Detect and Prevent



Downstream Victim Defenses

Netflow/Network Visualization analysis

- Most servers don't talk to other servers
- Most servers don't talk to workstations
- Most workstations don't talk to every server
- And so on
- Learn what is normal and alert on anomalous connections
  - Locations, Times, etc.
  - Large data copies off network or between servers
  - Unexpected piles of encrypted data sitting in unexplained places

How to Detect and Prevent

Downstream Victim Defenses

Netflow/ Network Visualization analysis

- Network traffic analysis tools
- Bro, Corelight
- Cisco
- ManageEngine Netflow Analyzer

- Look for a tool that does as much analysis as possible for you and alerts on anomalous traffic
- Hard part is getting technicians not to over-explain away new changes

How to Detect and Prevent

Downstream Victim Defenses

Netflow/ Network Visualization analysis

Alert on:

- Strange, unexpected, source to destination admin logons
- Example: Make a rule that domain admins can only logon to domain controllers and only from particular workstations and then alert on exceptions

How to Detect and Prevent

Downstream Victim Defenses

Privileged Group Analysis

- Attackers often add new accounts to privileged groups
- Alert on unexpected new memberships to privileged groups

How to Detect and Prevent

Downstream Victim Defenses

Honeypot Deception Technology

- Attackers don't know the difference between real and fake assets
- Alert on new connections to fake assets

KnowBe4 Security Awareness Training

Baseline Testing
We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

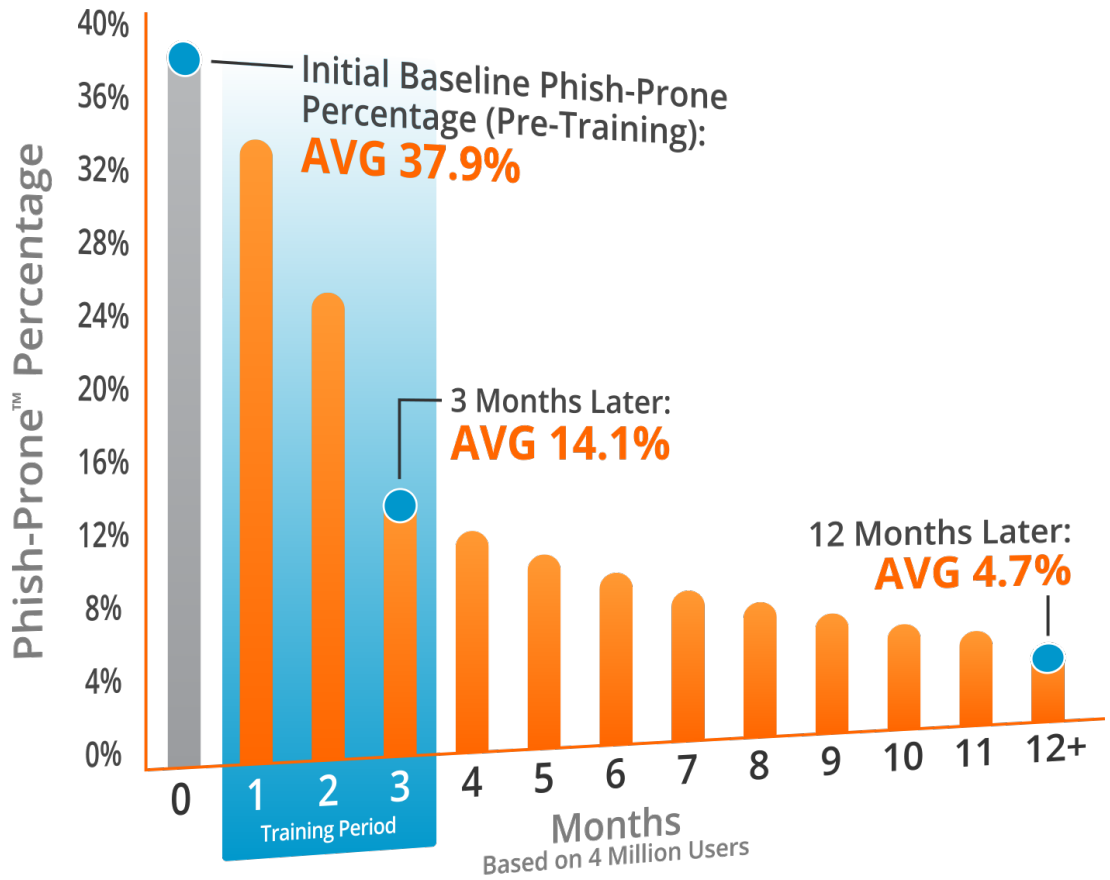
See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

Generating Industry-Leading Results and ROI

- Reduced Malware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

87% Average Improvement

Across all industries and sizes from baseline testing to one year or more of ongoing training and testing



Source: 2020 KnowBe4 Phishing by Industry Benchmarking Report

Note: The initial Phish-Prone percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 platform prior to the evaluation. Subsequent time periods reflect Phish-Prone percentages for the subset of users who received training with the KnowBe4 platform.

Questions?

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4
rogerg@knowbe4.com
Twitter: @rogeragrimes
https://www.linkedin.com/in/rogeragrimes/