Thursday, February 04, 2021 at 12:00 PM EST

SOLARWINDS

A SANS Lightning Summit

with Rob Lee, Katie Nickels, Mark Bristow, Mike Murr,
Evan Dygert, John Hubbard & Dr. Johannes Ullrich

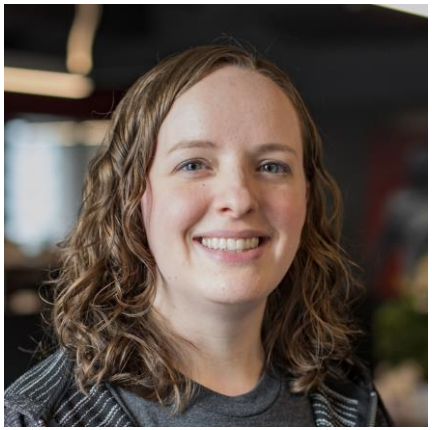
SANS

Key CTI Takeaways from “SolarWinds”

Katie Nickels
SANS Lightning Summit
February 4, 2021

red canary

About Me



- SANS Certified Instructor for FOR578: Cyber Threat Intelligence
- Bringing context about threats to inform decisions
- Maintaining sanity with exercise, chocolate, containers, and lights

Katie Nickels
DIRECTOR OF INTELLIGENCE
RED CANARY
@LiketheCoins

red canary

#1: It’s not a single compromise

red canary

Organizations affected

- FireEye
- SolarWinds
- Microsoft
- Palo Alto
- U.S. government agencies
- Cisco
- Mimecast
- Almost certainly others

#2: There are different names for good reasons

red canary

Incident names

- Solorigate – Microsoft
- SolarStorm – Palo Alto

Cluster and group names

- UNC2452 – FireEye
- Dark Halo – Volexity
- StellarParticle – CrowdStrike
- None of these teams attribute to countries!

Malware names

- SUNSPOT
- SUNBURST
- TEARDROP
- Raindrop
- SUPERNOVA
- COSMICGALE

red canary

#3: Threat models differ by organization

red canary

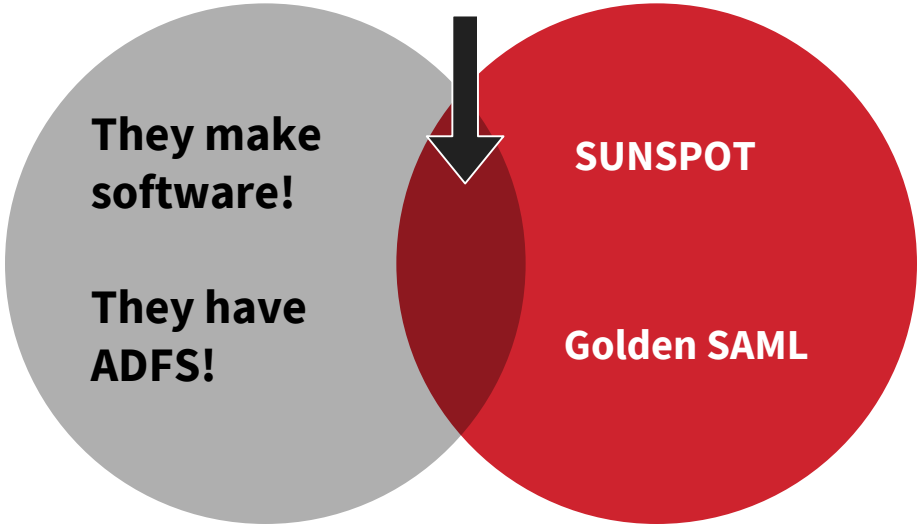
Think about your environment

- Do you use products/services from any compromised parties?
- Do you provide third party services to customers?
- Do you use cloud providers?
- Do you build software?

Identify the threats that matter to you

Prioritize validating their build process and detecting Golden SAML

A fictional software development company



All the SolarWinds-y threat things!

ATT&CK is a great starting place for looking at the threats

More on threat modeling

red canary

In summary

- Be specific when you talk about “SolarWinds”
- Remember there are different threats
- Carefully consider which aspects of these threats apply to you

Recommended compilation of references from MITRE: https://github.com/center-for-threat-informed-defense/public-resources/blob/master/solorigate/README.md

red canary

Thank you!

Katie Nickels

@RedCanary
@LiketheCoins

https://redcanary.com/blog/

red canary

SUPPLY CHAIN COMPROMISE

LESSONS LEARNED FROM THE FIELD

Mark Bristow

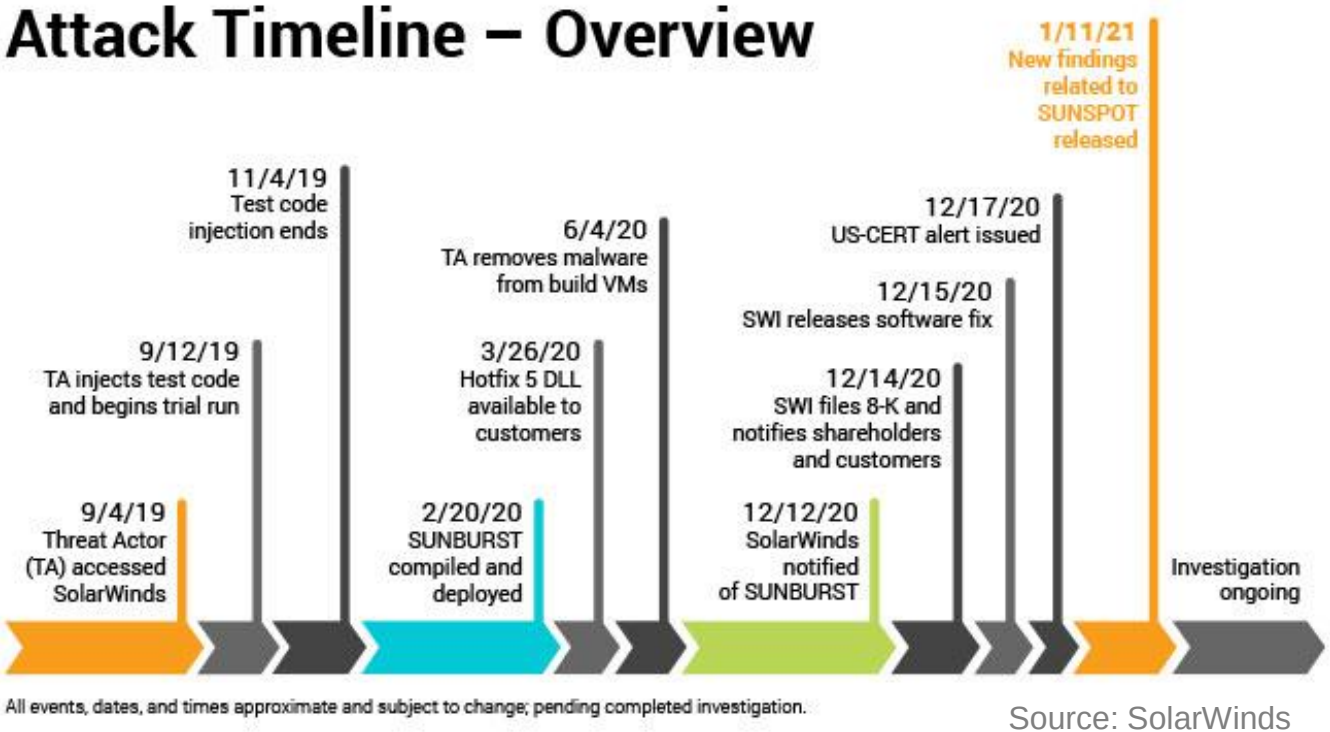
Branch Chief, Cyber Defense Coordination

CISA - Threat Hunting

Key Takeaways

- Patient, resourceful adversary
- The adversary is exploiting weaknesses in our supply chain and identity management
  - **It's not just SolarWinds**
  - Non-supply chain methods are being used
- Follow-on Actions on Objectives are very difficult for many organizations to identify
  - The targeting of incident responders adds new complexity

Supply Chain Attack Timeline



Source: SolarWinds

Identity is Everything

- Hosted/Cloud infrastructure and remote work drives this change forward
  - Identity is the new perimeter - “the firewall is dead”
- Trust store and IDM compromises are excellent targets that adversaries are exploiting
- Behavioral analysis techniques are required to identify an identity compromise

Detection Opportunities

- Detecting a supply chain compromise of this nature is beyond most organizations' capabilities
- Network baselining and abnormal behavior analytics are instructive
- User behavior abuse is best
  - Impossible Logins
  - SAML abuse
  - AA21-008A – Detecting Post Compromise Activity in Microsoft Cloud
  - Sparrow - https://github.com/cisagov/Sparrow

Key Questions to Ask

- Do you know who you trust? When did you last validate?
- Do you have visibility into your hosted/cloud environments? Can you see all authentication attempts?
- If your main network was compromised, can you operate?
- When did you last exercise your DR plan?

Points of Contact & Resources

- For reporting indicators of potential compromise, contact:
  - https://us-cert.cisa.gov/report
- For general questions and inquiries, contact:
  - central@cisa.dhs.gov
- CISA Supply Chain Activity Alerts:
  - https://www.cisa.gov/supply-chain-compromise


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

Malware Analysis Lessons from SolarWinds

Evan H. Dygert

Dygert Consulting, Inc.

SANS Certified Instructor

FOR610: Reverse Engineering Malware
SEC503: Intrusion Detection In-Depth
FOR508: Advanced Incident Response, Threat Hunting and Digital Forensics
SEC504: Hacker Tools, Techniques, Exploits and Incident Handling
SEC402: Cybersecurity Writing: Hack the Reader

Goals

- Show how malware analysis
  - provides the best source of knowledge of the sample.
  - helps create detection rules.
  - aids in decoding the DNS traffic.

Triage

- Easily decompiled .NET DLL.
- Many obfuscated strings.
- Some code obfuscation (e.g. misleading names).
- Decoded strings clearly suspicious.
- Many "timestamps" that clearly were not timestamps.

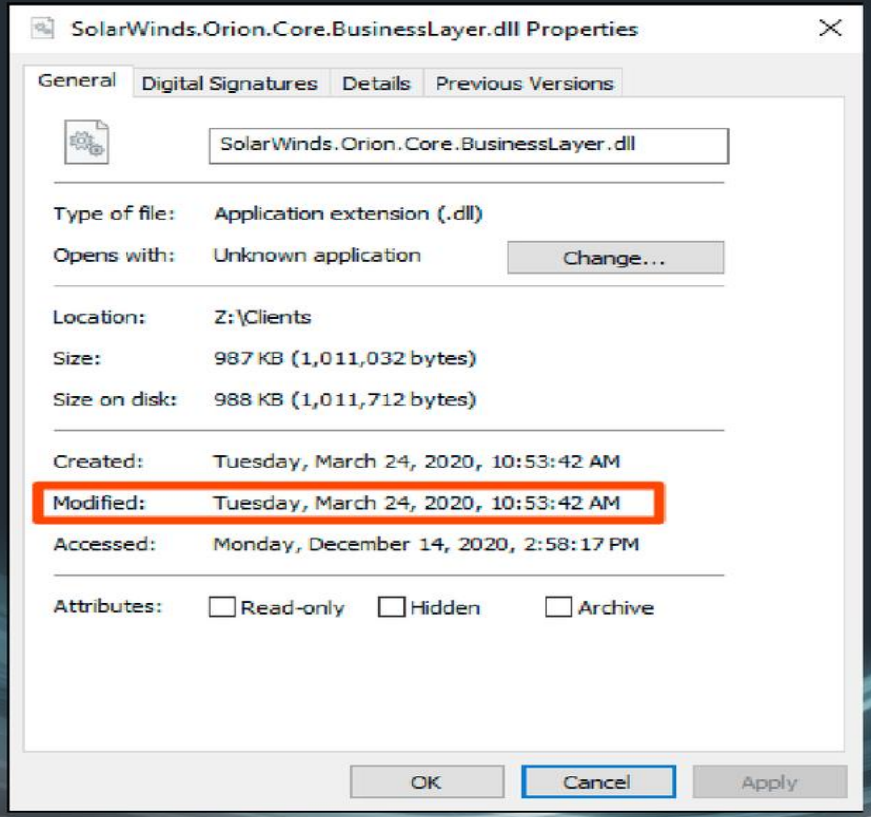
OrionImprovementBusinessLayer.Initialize

- Runs every time the InventoryManager.Refresh function runs (if it's not currently running).
- Performs various checks before the malware runs.
- Reports of how the delay check works were generally incorrect.

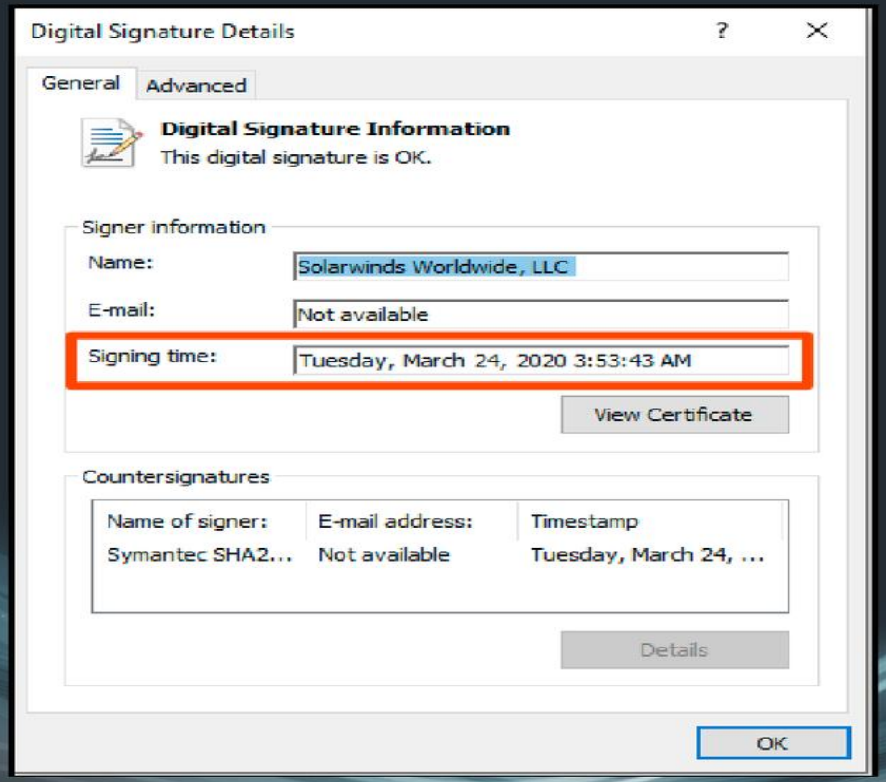
Delay

- The code does contain a delay of 12-14 days.
- But what date is the delay measured from? Installation or compilation or ...?
- The delay was measured from the last modified date of the DLL, but what is that date?

Last Modified Date



Signing Date



Delay (cont.)

- It is NOT the date of installation but of compilation.
- The compilation date is preserved as the last modified date by the installation program.

But What Does This Mean?

- The delay does not protect the backdoor from sandboxes as widely reported.
- You can not assume the malware did not run if it has only been on your system for a few days.
- Assuming the other checks pass, the malware will run.
- Unknown if this is a bug or if the delay was meant to prevent the malware running during the QA period.
- FOR610 & FOR508 for the win!

Detecting Changes to Services

- The backdoor disables services by changing the registry.
- Changes do not take effect until machine is rebooted.
- Sysmon, for one, can monitor these kinds of changes.
- You may catch other malware that disables services or changes other sensitive parts of the registry.
- See SEC511: Continuous Monitoring and Security Operations for lots more about this topic.

DNS Traffic Decoding

- No public scripts completely decoded the DNS traffic.
- Decoding for stage 2 was incorrect.
- We reverse engineered the code to get it right.

DNS Requests

- Up to 16 DNS requests were used to transfer long host/domain names.

Data Sent in DNS Requests
host id
timestamp
encoded host/domain name
installed/running status of security products
if the backdoor had seen "request 2" response

Conclusions

- Use malware analysis to really understand the malware.
- Combine MA with digital and network forensics.
- Do your own analysis if possible. You just may be surprised at what you find!

References

- https://blog.reversinglabs.com/blog/sunburst-the-next-level-of-stealth
- https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html
- https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html
- https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/
- https://news.sophos.com/en-us/2020/12/21/how-sunburst-malware-does-defense-evasion/
- https://blog.prevasio.com/2020/12/sunburst-backdoor-part-iii-dga-security.html
- https://github.com/ITAYC0HEN/SUNBURST-Cracked

SolarWinds

Best and Worst Organizational Approaches to IR

socialexploits

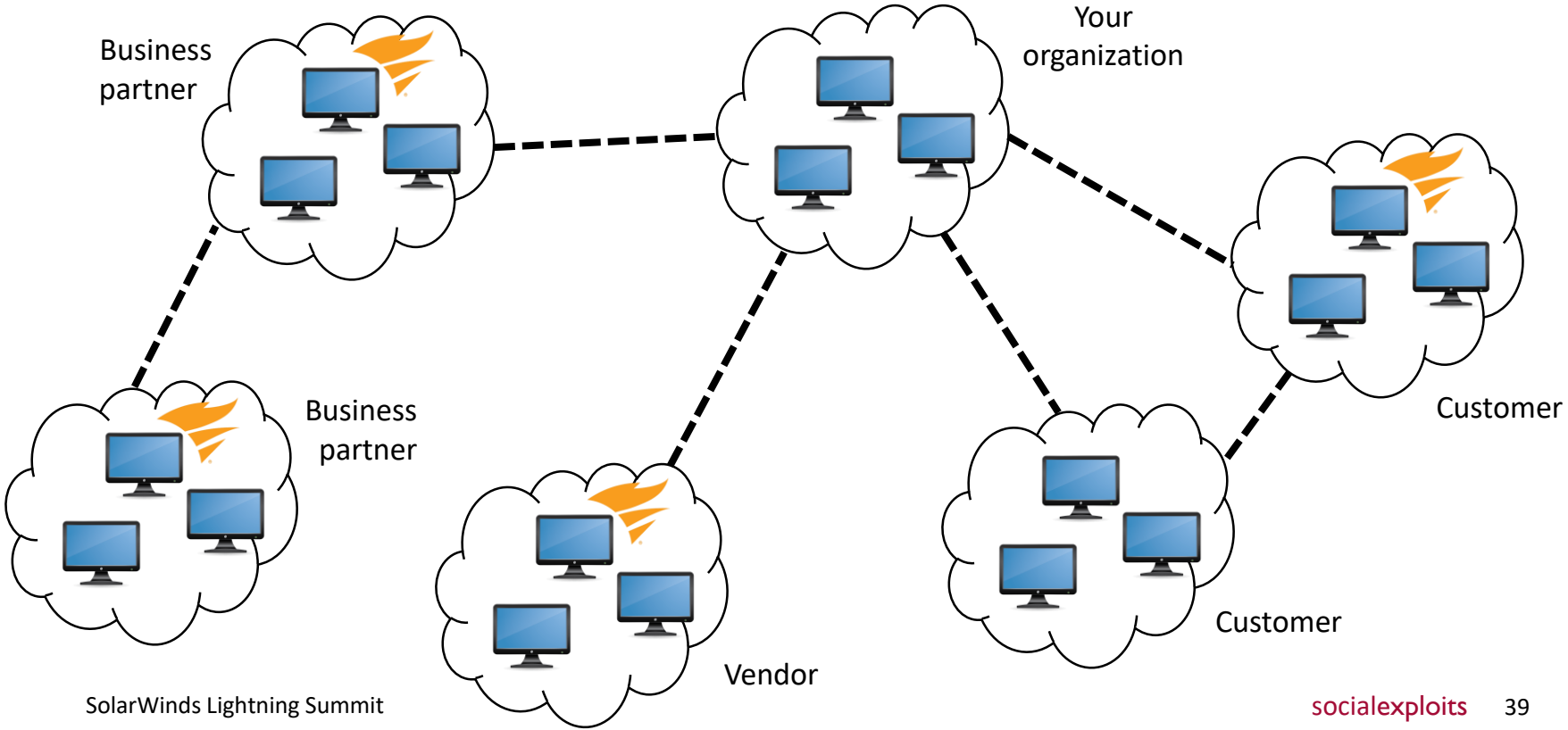
Mike Murr | Sr. Consultant

Principal Instructor @ SANS

What's Happening ... But Not Working

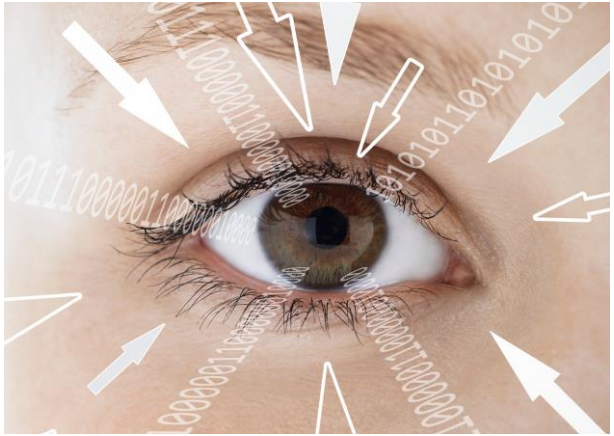
- We don't run SolarWinds
  - What about your supply chain?
  - 30% of victims weren't running SolarWinds
- Ignoring the problem
  - We're not a target
  - We don't update (they have bigger problems)
- Improper scoping
  - Scan, find implant, remove, done
  - Apply patches, done
  - Block domains, done

Your Business Is More Than You



Perspective Shifts that Work

- Your risk boundary is not your network boundary
  - Think *business ecosphere* not just network
  - Consider the risk vendors pose ...
    - They are a part of your risk
    - What data do they have that is *your* liability?
  - Who are you a vendor to?
- Plan for compromise
  - This incident highlights one single point of failure
  - Tabletop exercise “impossible” scenarios
  - What would cause your business to fail?
    - Not just your network
- Legitimate business processes were attacked
  - Plan like any corporate-wide change
  - It’s going to be a long-term IT project



Specifics That Work

- Know your environment
  - Hardware, software, vendor-supplied
  - Versions, configurations, changes
  - Examples
    - Domain controller at an offsite
    - Vendor installed ADFS as a requirement
  - Not easy, but attackers will know it
- Make sure you log
  - Especially DNS
- Make sure you can access logs
  - High-volume logs age quickly
  - O365 and Azure can be problematic

References

- Titles on slide, full citations in notes
- Suspected Russian Hack extends far BEYOND SolarWinds Software, Investigators say
  - https://www.wsj.com/articles/suspected-russian-hack-extends-far-beyond-solarwinds-software-investigators-say-11611921601
- Disrupting Nation State Hackers
  - https://www.usenix.org/conference/enigma2016/conference-program/presentation/joyce

SANS Institute

SolarWinds:
Blue Team Perspective & Opporunties

John Hubbard

@SecHubb

Tactics Summary – Why This Was So Difficult

- **Delivery**: Supply chain attack - trusted vendor
- **Execution**:
  - Living off the land / legitimate tool usage
  - Malicious scripts and DLLs
- **Persistence**: WMI and registry keys
- **Command and Control:**
  - Domain generation algorithms and HTTPS for C2
  - *Very* well-hidden encoded data in HTTP request body
- **Exfil**: Compressed, encrypted, broken-up archives
- **In general**: Unique EVERYTHING
  - Literally, everything – files, folders, hashes, domains, WMI filter names, reg keys, and more

Execution

Tactic: Living off the Land / Legitimate Binaries

- *AdFind* software by Joeware was used for Discovery
- Command line querying of active directory details
- Used hidden in non-standard locations / names for applications

Opportunities for Detection:

- ❑ Direction detection of AdFind in any form – quite unusual
- ❑ Execution of AdFind by unexpected *person*
- ❑ Execution of AdFind Hash by a file *not* named "AdFind"
- ❑ AdFind executed from *non-standard location*, detected by hash
- ❑ Unique executables by file name

Execution

Tactics: Execution via scripts and DLLs

- SUNBURST drops VBS script and DLL in C:\Windows\[folder]\
- Wscript launches VBScript file
- VBScript calls Rundll32 to run malicious DLL (Cobalt Strike Loader)

Opportunities for Detection:

- ❑ Application control for scripts and DLLs (AppLocker)
- ❑ Process command line and argument logs to identify unique/suspicious wscript arguments
- ❑ Scripting logs where available (PowerShell logging)
- ❑ Script execution unique to a single machine
- ❑ First time script execution / frequency of execution
- ❑ Monitoring for unsigned DLLs or unique signed executables

Persistence

Tactics: Persistence via WMI Filters and Windows registry-based persistence

- Registry key addition for Image File Execution Option debugger (IFEO)
- WMI event filter used to launch event consumer that ran Rundll32 at boot

Opportunities for Detection:

- ❑ Monitoring for *suspicious* ASEPs
- ❑ Monitoring for *unique* ASEPs
- ❑ Monitoring for *change* of ASEPs Unique WMI filter names monitored via Sysmon, etc.
- ❑ Monitor IFEO registry keys for changes, abnormal process parent/children
- ❑ Tools: Autoruns, Windows object access auditing, EDR, and more

Defense Evasion

Tactics: Living off the land with built-in Windows commands

- Auditpol run to disable logging
- Firewall rule modification via netsh commands
- Disabling of security services before lateral movement

Opportunities:

- ❑ Detection of disabling / attempting to disable security services
- ❑ Execution of auditpol – detect via HIDS/HIPS
- ❑ Questionable commands (netsh) run from non-IT users
- ❑ Network-based monitoring for unexpected traffic origins and types
- ❑ Baseline config monitoring for changes

Command and Control / Defense Evasion

Tactic: DGA for command and control (___.___.avsmcloud.com)

- Used random looking subdomains for connections
- IP addresses used from within victim's country (all same ASN)

Opportunities for Detection:

- ❑ Domain new to your org
- ❑ Domain unique to a single (or few) machines
- ❑ Domain with unknown reputation
- ❑ High entropy in subdomain
- ❑ Many subdomains per parent level domain (DNS tunneling)
- ❑ Detecting login attempts from a new ASN

Exfil

Tactics: File hiding

- Compressed, encrypted archive creation
- Used renamed standard tools (7zip)

Opportunities for Detection:

- ❑ 7z archive creation with passwords (cmd line)
- ❑ Breaking files up into pieces (cmd line)
- ❑ Using non-7z file extensions for archives
- ❑ 7zip detected under alternate name, non-standard location

General Approach for Catching Future Complex Attacks

When you DO know about a tactic/tool

- Write a detection to highlight its use
- Exclude standard usage of that program (admin tool use)
- Look for non-standard details, users, locations, names

Microsoft blog post: sec450.com/sunburst

When you DON'T know what something will look like

- Looking for *anomalies* in all ways
- A single machine or user running a new program
- "First contact" rules for domains, scripts, and more
- Newly created domain access, first time access for domain

Beyond SolarWinds

- SolarWinds combined some attack patterns we have seen individually before:
  - Advanced Adversary
  - Supply Chain Attack
  - Long dwell time
  - Impacted many organizations
- It was “special” because it combined all of these in one attack.

My Classes:

- SEC503 Intrusion Detection in Depth
- SEC522 Defending Web Applications

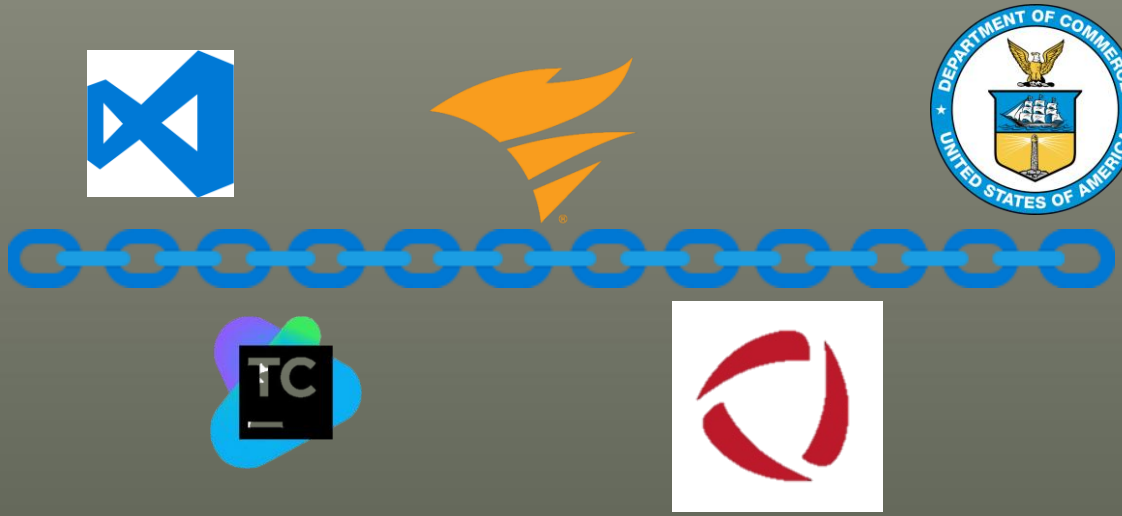

jullrich@sans.edu


@johullrich

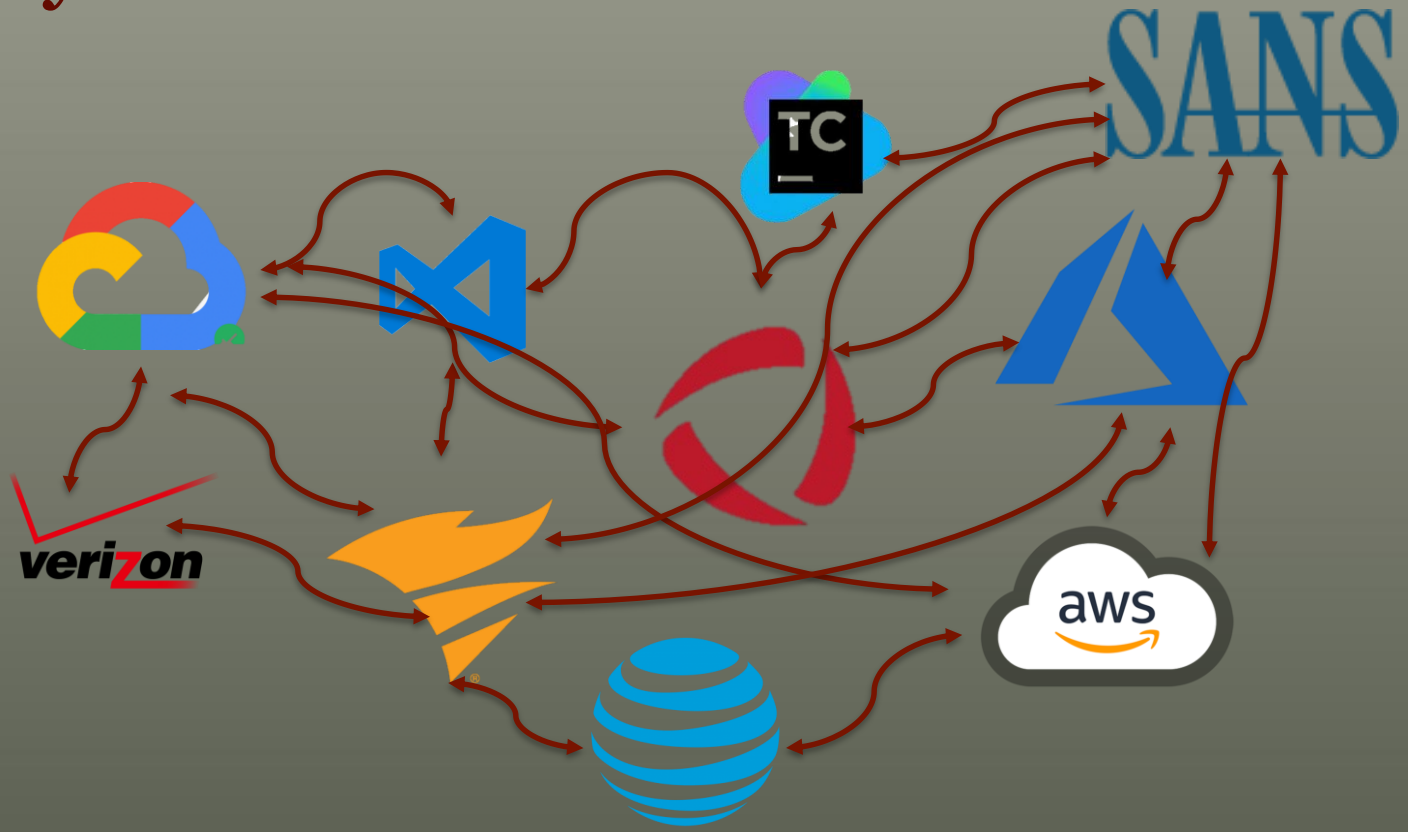
SANS Technology Institute

Supply Chain

Software Tools	Developer	User

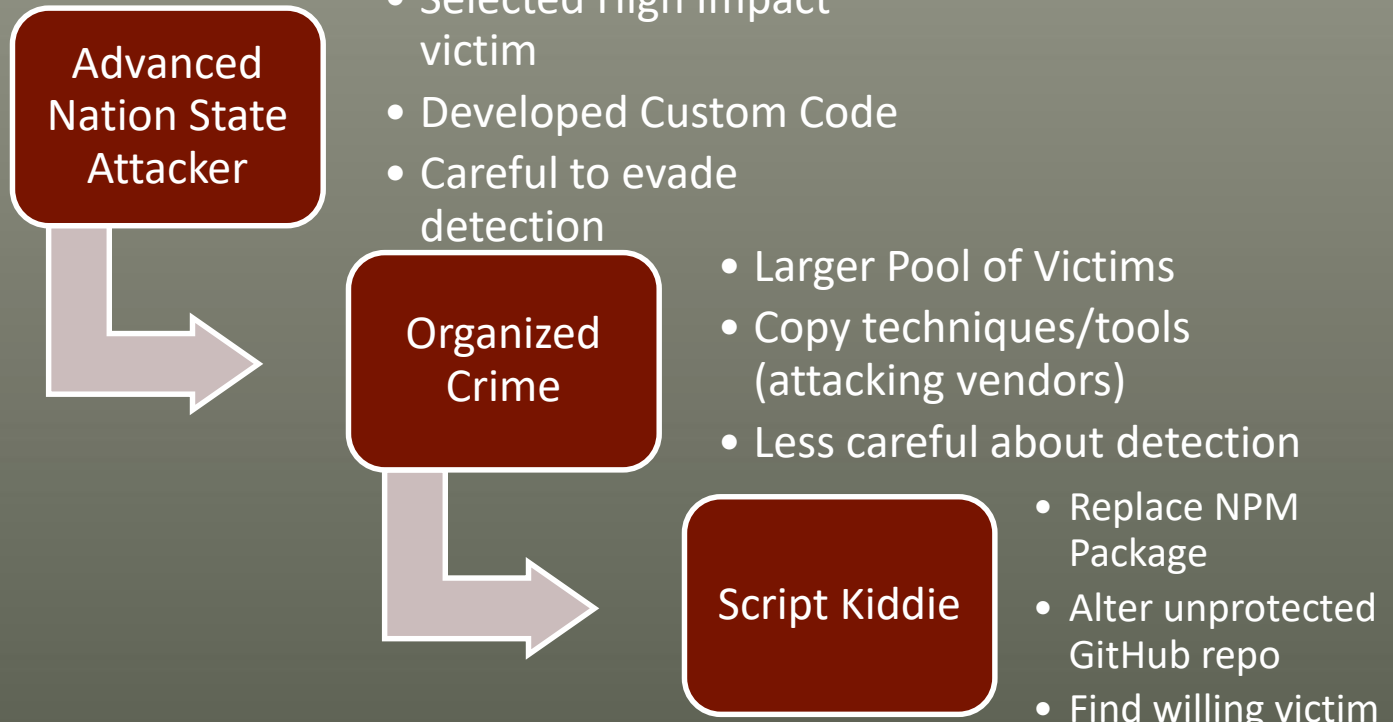


Supply ~~Chain~~ Network



SANS Technology Institute

Expect Next: Others will take notice/copy



SANS Technology Institute

Detecting the Next SolarWinds

- STOP looking for IOCs
  - Zeek: Big winner from SolarWinds post-mortem
  - Know your network
  - Anomalies / long tail analysis
  - Build capability to detects TTPs not IOCs
  - SHARE!

SANS Technology Institute

Preventing the Next SolarWinds

- Protect and Monitor your Software Development Pipeline
  - Software Bill of Materials (SBOM)
    Yes, it is difficult. But it doesn't get easier if you wait.
  - Static security analysis of 3rd party code / libraries
    Avoid "blind trust" in components
  - Bake security into development process
    It will not happen if you do not automate and test it.

SANS Technology Institute