POINT
OF VIEW

Recorded Future®

By John Wetzel

POV-2020-1230

SOLARWINDS ATTRIBUTION:

Are We Getting Ahead of Ourselves?

An Analysis of UNC2452 Attribution

Note: A previously version of this report incorrectly attributed disclosure of Jake Williams' work for the National Security Agency's Tailored Access Operations group to Sandworm. This disclosure was conducted by ShadowBrokers.

Overview

The recent expansive intrusion campaign of over half a dozen government agencies and as-yet unknown other organizations through malicious backdoors in the SolarWinds Orion platform is already one of the most significant acts of cyber espionage in history. This intrusion, dubbed SUNBURST/Solorigate, appears intended for information theft and espionage rather than destruction, placing this campaign within the realm of counterintelligence, not just incident response. Analyzing this incident within the realm of counterintelligence may fill the gap of descriptive language for this incident rather than bipolar descriptions of "sophisticated" or in-depth analysis which may add to confusion for network defenders. Additionally, only a handful of companies have direct access and the investigative resources to gain meaningful insights into the technical components of the backdoor. The actor is a different story.

Like most complex, public intrusions, attribution has been messy. FireEye has named the actor behind this intrusion "UNC2452," and Volexity dubbed the threat actor "Dark Halo," stating that the actor is the same as UNC2452, though FireEye has not substantiated that claim. Adding further complexity, Washington Post correspondent Ellen Nakashima cited unnamed government sources claiming Russian actors, in particular APT29, are responsible for the attack. Members of the U.S. Congress have also publicly accused Russia, and in particular the Russian Foreign Intelligence Service (SVR), as the responsible party, and added calls for response. Microsoft President Brad Smith has also called for strong action. While we expect these organizations have far more insight into the nature of the breach, as well as classified sources of intelligence information, calls for strong response should include publicly disclosed information to support accusations.

Public evidence for these claims is currently scant. Some, including Jake Williams, who runs Rendition Security and teaches for the SANS Institute, has said that technical evidence is forthcoming, but cannot be disclosed without tipping off the adversaries to missteps and giving them a means to cover their tracks. Still, the lack of public evidence gives rise to claims that other actors, even perhaps other countries, may be responsible, a claim made by President Donald Trump as well.

Intelligence analysis, properly conducted, combats bias. Bias can lead to missteps in policy. Engaging in policy discussions about proportional responses (or, at times, very disproportionate response) without strong evidence is potentially dangerous. As rumors of attribution to Russia circulate, attribution prior to evidence is premature and myopic, biasing the analyst to only certain behaviors and actors. Further, intelligence analysis provides both strategic and tactical guidance for responses. At the strategic level, we can be assured that responses are coordinated and proportional. At the tactical level, defenders can apply intelligence to seed proactive activities, such as hunting for behaviors after indicators run dry.

Among information security researchers, some discussion has occurred regarding the possibility alternate actors, such as APT41, may ultimately be found responsible. APT41, also known as Winnti and Barium, has been linked to the People's Republic of China, and previously conducted attacks which beg comparison with the SUNBURST/Solorigate attack. (Note: Recorded Future has synonymized several named groups, including APT41, Axiom Hacking Group, Barium, Blackfly, Dogfish, Ragebeast, Wicked Panda, Winnti Group, as Winnti Umbrella Group.) In March 2017, APT41 executed a supply chain attack by breaching the company which made CCleaner, a system cleaner software. Researchers from Cisco Talos and Morphisec uncovered the campaign, which ultimately spread to 2.27 million computers. While these comparisons fall well short of the requirements for attribution, APT41 does merit consideration as a candidate actor group responsible for the SUNBURST/Solorigate breach. Enter threat intelligence.

Noteworthy Techniques

We approached our analysis using existing techniques in order to focus on attribution and adversary mapping. We pursued methodologies including mapping MITRE ATT&CK techniques, victimology, temporal indications, and historic use of indicators to give insight into attacker motivation and intent. We analyzed both public information as well as information from Recorded Future's historic index to determine a set of unique characteristics about this campaign. Our goal was not to conclusively attribute this attack, but rather to review existing data through the lens of intelligence analysis and contribute to conversation on adversary tracking.

ATT&CK Technique Analysis

We conducted a comparison of ATT&CK techniques across the mentioned actors, including APT29 and APT41. We compiled 25 techniques and 14 sub-techniques for UNC2452 using MITRE ATT&CK Matrix for Enterprises and techniques mentioned in public reports from FireEye and Microsoft. We then used the MITRE guidance for comparison of groups, and compared UNC2452 ATT&CK techniques against those the MITRE team documented for APT29 and APT41 using ATT&CK Navigator (Appendix). Unfortunately, our analysis surfaced several challenges.

First, there are significant differences in documented ATT&CK techniques between vendors analyzing the same actor group and/or malware. For example, FireEye lists seven techniques and 10 sub-techniques in their report dated December 13, 2020; Microsoft shows four techniques and six sub-techniques for their report dated December 18, 2020.

Second, several techniques for APT29 and APT41 were missing from the ATT&CK groups cataloged by MITRE, appearing to lean towards more recent attacks, such as PowerDuke campaigns. We used MITRE's maintained list of APT TTPs for initial comparison, however these appear to have notable gaps even malware techniques and techniques for actor groups attributed to leverage the malware.

Third, there were specific instances where ATT&CK lacked the nuanced matching techniques described by security reporting. For example, within ATT&CK Navigator, several techniques are automatically assigned to tactics, such as T1078 Valid Accounts, which is assigned to Initial Access, Persistence, and Defense Evasion tactics. While Microsoft does cite this technique, they limit its applicability to the Persistence tactic.

Additionally, some techniques gain meaning through both repeated applications and choices of what to encode. A salted FNV-1a hashing algorithm is used in both encoding blacklisted domains and blacklisted processes, corresponding to T1132 Data Encoding. However, the domains hashed with FNV-1a are also used to standardize various components of information in checks prior to downloading the second-stage payload, creating efficiencies for communication as well as obfuscation.

While ATT&CK is a strong framework for mapping adversary TTPs, it is missing elements critical to describe ongoing adversary activity and map that activity to past activity. Vendor publication of ATT&CK techniques without in-line context further reduces applicability to adversary mapping. Historic activity tracking can provide insights into both the existing, and potentially ongoing, SUNBURST/Solorigate campaign and clues to actor motivation and attribution.

Victim Scope

Victimology, in particular, is notable for UNC2452, as it demonstrates an exacting approach to preserving continuity of operations while prioritizing victims. As reported in a statement from Microsoft President Brad Smith, of approximately 18,000 organizations who received the SolarWinds update containing the backdoor, only 0.2 percent received the second stage, and 40 of those companies, 80 percent of the chosen companies, were located in the United States. According to FireEye, adversary use of domain generation algorithms (DGA) custom to each victim allowed for various organizations to identify organizations beaconing to the backdoor Command-and-Control (C2) server through passive DNS records and cracking the encoded subdomains.

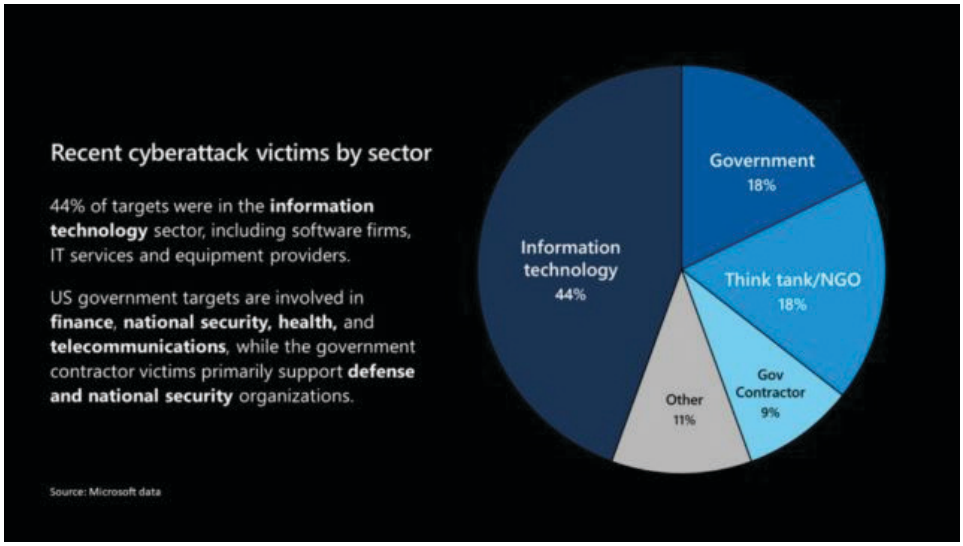


Figure 1: Microsoft graph of victims by industry sector. (Source: Microsoft)

The plurality of victims, according to Microsoft, are information technology companies. While much of the media coverage remains on government and government contractor victims, recent reports of victims from telecommunications providers to healthcare organizations, demonstrate targeting beyond traditional espionage targets.

Some victimology can be determined through the reversing the DGA used by the Solorigate backdoor. Several organizations, such as the RedDrip Team, Netresec, and Kaspersky published methods for decoding the DGA used by the backdoor for initial C2 communications. Recorded Future collected and combined information gathered from open sources such as Pastebin, passive DNS datasets (pDNS), and others related to encoded subdomains of the SolarWinds Orion backdoor first stage command and control (C2) domain avsvmcloud[.]com, and utilized three DGA decoding scripts. As of December 21, 2020, we have identified some 286 domains.

> ***This output is the result of a small subset of open source data and is not representative of the totality of affected organizations, and is based exclusively on Recorded Future's visibility at this time via open source datasets. SolarWinds itself has said that roughly 18,000 organizations installed versions of SolarWinds Orion software impacted by SUNBURST, so the list of identified domains by Recorded Future is therefore non-comprehensive. Additionally, an organization's presence on this list does not necessarily mean that it is the victim of second stage infection or data exfiltration. Specific conditions had to be met for the malware to deploy a second stage. We do not currently have visibility into further exploitation. Not all of the records are complete domains; we have included partial or incomplete domains where we deemed that there was sufficient enough information to make educated guesses or inferences as to which organization the domain or string may reference.***

Microsoft noted in its report that the malware checks domains for certain strings prior to execution, but was not able to determine the domains as they were implemented via hashes. Itay Cohen, a security researcher at Checkpoint, identified the strings as FNV-1a hashes, and was able to brute-force reverse them. Cohen noted that many of the strings appear to be SolarWinds internal domain names. In combination with the checks conducted by the malware to look for regular expressions of "solarwinds" and "test", Cohen posited the attackers gained intimate knowledge of the SolarWinds source code, as well as the network topology and internal development domain names, in order to "minimize the risk that a vigilant employee will notice the anomaly." Costin Raiu, along with another Kaspersky researcher, cracked the remaining hashes and published the full list of internal domain names. Such care to avoid detection is highly uncommon, and points towards an impressive degree of reconnaissance and focus.

```
OrionImprovementBusinessLayer.patternHashes = new ulong[]
{
    //HASH                    //domain:
    1109067043404435916UL,    //[dev.local]
    15267980678929160412UL,   //[swdev.dmz]
    838129226599397726 6UL,   //[lab.local]
    379640562369566552 4UL,   //[lab.na]
    872747776954430206 0UL,   //[emea.sales]
    107341270042448797 70UL,  //[cork.lab]
    110732833111045416 90UL,  //[dev.local]
    403023641397519965 4UL,   //[dmz.local]
    770168327982439777 3UL,   //[pci.local]
    513225662010499863 7UL,   //[saas.swi]
    594228205252529491 1UL,   //[lab.rio]
    457848084625562946 2UL,   //[lab.brno]
    168589559781464066 42UL   //[apac.lab]
};
```

Figure 2: FNV-1a hashes and the resulting domain names avoided by the SUNBURST malware.

Subsequently, SentinelOne found that SUNBURST also appears to check for certain running processes, and exits if these processes are discovered:

> *"SearchConfigurations() is used to identify blacklisted drivers. This is performed through the WMI query – Select * From Win32_SystemDriver, which is obfuscated in the below screenshot as C07NSU0uUdBScCvKz1UIz8wzNooPriwuSc11KcosSy0CAA==. The file name is obtained for each driver, and if this driver is found in the blacklist, this method will return true. As mentioned before, returning true causes the malware to break out of the Update() loop prior to initiating the true backdoor code."*

Among the blacklisted processes are a number of digital forensics and endpoint detection and response tools. A full list of the drivers can be found on the SentinelOne blog. Similar to the Microsoft revelation of blacklisted domains, this care to avoid endpoint detection again highlights the cautiousness of the actors.

Additionally, analysis is needed on the list of SUNBURST blacklisted processes. The full list was cracked by several open source researchers. A public Google Sheet was compiled by Royce Willams and the Hashcat team. The list of blacklisted processes is not comprehensive of all common endpoint or antivirus vendors; further analysis is required to understand why the malware authors focused on certain endpoint software to blacklist.

Time

A unique feature of the Solorigate backdoor is the timestamp check that the last write time for the DLL was 12-14 days prior. Even among unique malware samples, this duration is atypical. MITRE ATT&CK lists a few attackers leveraging this technique, and none approaching this level of time, but this may be due to incomplete documentation within ATT&CK, as mentioned above. In addition to evasion, the time-based evasion appears to be more related to avoiding detection by SolarWinds staff rather than analysis through virtualization/sandbox analysis.

In a broader examination, the campaign appears to have breached SolarWinds in the fall of 2019 and made non-malicious changes to code. These changes amounted to a dry-run of the primary infection which would occur around March 2020. Additionally, the actors inflated the size of the targeted DLL file from 500k to 900k, which may have triggered detection rules for the file, but investigations would have turned up no malicious code. When infected code was added in February/March 2020, the size increase was minimal. Time to conduct these preparatory actions over the course of months shows a level of discipline and patience seen primarily in intelligence collection operations.

Historic Indicators

Multiple indicators have been shared by FireEye and in other vendor reports. While a number of these indicators are novel to this attack, Recorded Future does have historic references to some of these indicators.

Recorded Future sees historic collection on three domains from this report:

- The domain freescanonline[.]com was first seen in a ReversingLabs scan on November 28, 2017, associated with the following SHA256 hash: 21bab0d279d15a548a84a9d9eed34575b2dc9072cc36ebfe7b517850eea92756.
- The domain also appeared in an additional ReversingLabs scan on October 13, 2019 was associated with the SHA256 hash: c5864330c247e2cd2a98d69b852e42f59a16d9613a6536c8b0b25e16c934533d.
- The domain highdatabase[.]com appears publicly on a public Pastebin site with the title "NII GSOC Advisory", posted December 10, 2020.

Of 10 IP addresses noted in the FireEye report, only three were previously linked to malicious activity.

- 13[.]59[.]205[.]66 first appeared on Pastebin in February 6, 2018, and then appeared as a malicious host by a URLScan listing on April 23, 2019: https://urlscan.io/result/3df2efd6-530f-4973-bca7-4635c083e276
- 139[.]99[.]115[.]204 was mentioned in two URLScan results dating back to June 2019. In December 2019, this IP address was mentioned in a report by NAO_sec, associated with a tool they named Bottle Exploit Kit, targeting Japan, and associated with the domain sales[.]inteleksys[.]com
- 167[.]114[.]213[.]199 previously listed on the Bambenek list as a DGA domain destination. Additionally, Recorded Future's Predictive IP Risk Rule triggered for this IP days prior to announcements of the SolarWinds incident

In addition to the techniques mentioned by FireEye, in its report dubbing the backdoor "Solorigate," Microsoft attributed the five additional techniques and one sub-technique to the campaign:

Execution

- T1072 Software Deployment Tools

Command and Control

- T1071.004 Application Layer Protocol: DNS
- T1132 Data Encoding

Defense Evasion

- T1480.001 Execution Guardrails: Environmental Keying
- T1562.001 Impair Defenses: Disable or Modify Tools

Collection

- T1005 Data From Local System

DomainTools has published two blogs approaching the topic from the perspective of publicly available DNS records. In addition to documenting the DNS records published by FireEye, they also published additional domains used for the delivery of the second-stage payload.

Domain	Create Date	IP	Hosting Provider	SSL/TLS Certificate
databasegalore.com • 69	2019-12-14	5.252.177.21 • 79	MivoCloud SR	d400021536d712cb
digitalcollege.org • 75	2019-03-24	13.57.184.217 • 27	Amazon Technologies Inc.	fdb879a2ce7e2cda2
ervsystem.com • 10	2018-02-04	198.12.75.112 • 5	ColoCrossing	0548eedb3d1f45f1f
globalnetworkissues.com • 72	2020-12-16	18.220.219.143 • 72	Amazon Technologies Inc.	ff883db5cb023ea6b
incomeupdate.com • 72	2016-10-02	5.252.177.25 • 78	MivoCloud SRL	4909da6d3c809aee
infinitysoftwares.com • 5	2019-01-28	107.152.35.77 • 0	ServerCheap INC	e70b6be294082188
kubecloud.com • 69	2015-04-20	3.87.182.149 • 73	Amazon Data Services NoVa	1123340c94ab0fd1
lcomputers.com • 74	2002-01-27	162.223.31.184 • 5	QuickPacket LL	7f9ec0c7f7a23e565
panhardware.com • 74	2019-05-30	204.188.205.176 • 79	SharkTech	3418c877b4ff052b6
seobundlekit.com • 74	2019-07-14	3.16.81.254 • 73	Amazon Technologies Inc	e7f2ec0d868d84a33
solartrackingsystem.net • 73	2009-12-05	34.219.234.13 • 0	Amazon Technologies Inc.	91b9991c10b1db51
virtualwebdata.com • 73	2014-03-22	18.217.225.111 • 72	Amazon Technologies Inc.	ab93a66c401be78a
webcodez.com • 73	2005-08-12	45.141.152.18 • 5	M247 Europe SRL	2667db3592ac3955
zupertech.com • 74	2016-08-16	51.89.125.18 • 78	OVH SAS	d33ec5d35d7b0c23

Figure 3: Screenshot of DomainTools domains used in follow-on stages, enriched with Recorded Future Express Plus Browser Extension (December 20, 2020).

Of these second-stage domains, several appear in our index with significant delays between domain registration and certification registration references.

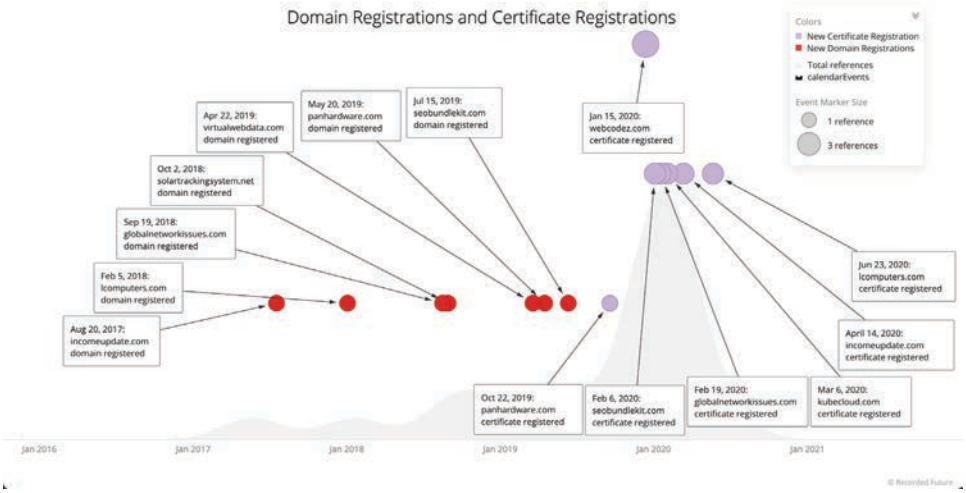


Figure 4: Timeline of the domain registration and certificate registration delay. (Source: Recorded Future)

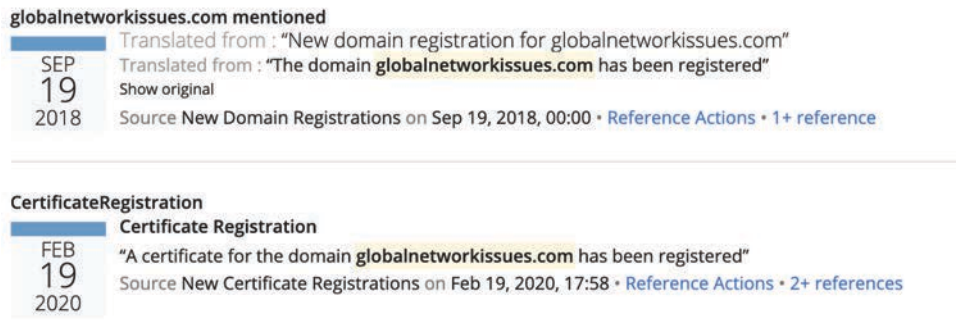


Figure 5: References showing the domain registration and certificate registration dates for globalnetworkissues[.]com domain. (Source: Recorded Future)

We note the registration of globalnetworkissues[.]com on September 19, 2018, however we do not see a TLS certificate registered for this domain until February 19, 2020, 17 months to the date later.

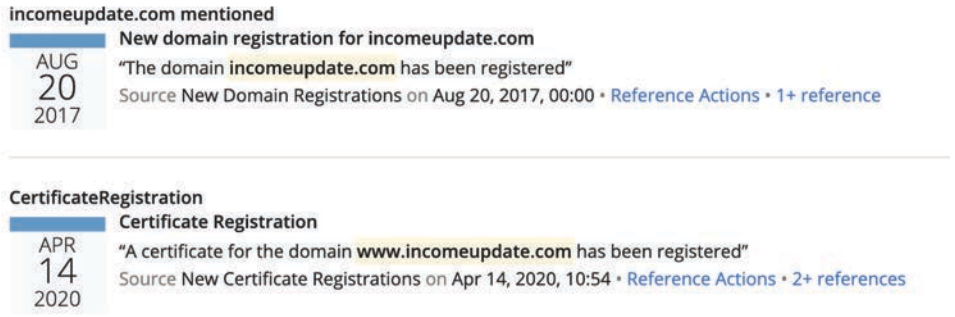


Figure 6: References showing the domain registration and certificate registration dates for incomeupdate[.]com domain. (Source: Recorded Future)

We see the registration of incomeupdate[.]com on August 20, 2017, but do not see a TLS certificate registered until April 14, 2020, almost 19 months later.

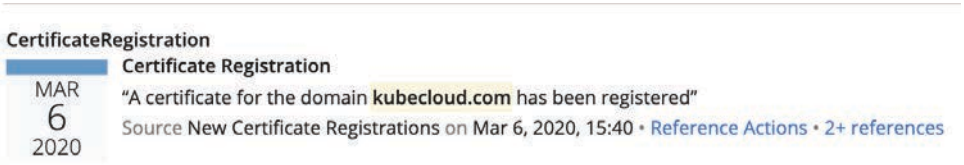


Figure 7: Reference showing the certificate registration dates for kubecloud[.]com domain. (Source: Recorded Future)

We see a TLS certificate registration for kubecloud[.]com on March 6, 2020.

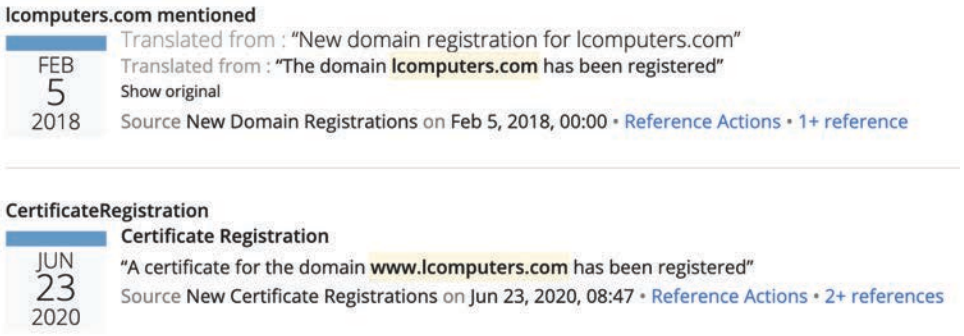


Figure 8: References showing the domain registration and certificate registration dates for lcomputers[.]com domain. (Source: Recorded Future)

We see the registration of lcomputers[.]com on February 5, 2018, but do not see a TLS certificate registered until June 23, 2020.

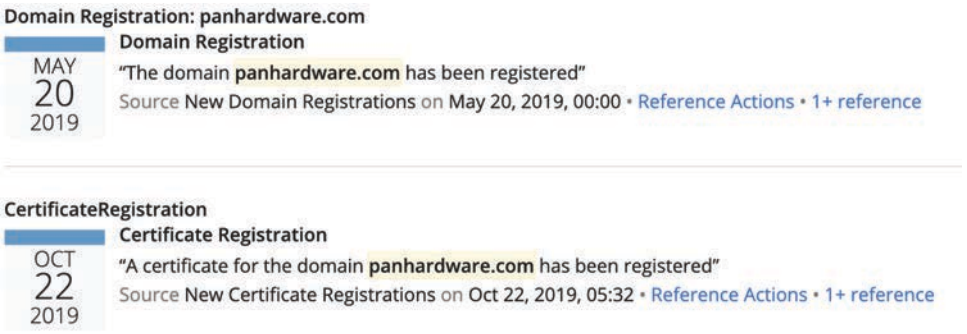


Figure 9: References showing the domain registration and certificate registration dates for panhardware[.]com domain. (Source: Recorded Future)

We see the registration of panhardware[.]com on May 20, 2019, and see a TLS certificate registered on October 22, 2019, five months later. This registration so much prior to the other second-stage domains is interesting and worthy of further investigation.

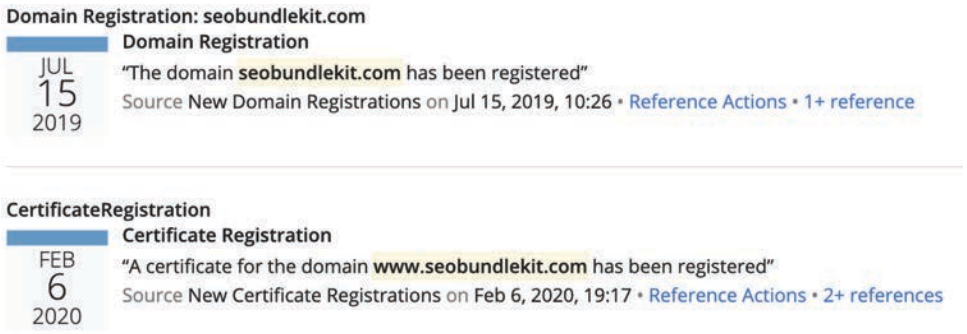


Figure 10: References showing the domain registration and certificate registration dates for seobundlekit[.]com domain. (Source: Recorded Future)

We see the registration of seobundlekit[.]com on July 15, 2019, but do not see a TLS certificate registered until February 6, 2020.

Figure 11: Reference showing the domain registration date for solartrackingsystem[.]com domain. (Source: Recorded Future)

For this domain and the next two domains, we see a reference to either a domain registration or a certificate registration, but not both. For this reference, we see the registration of solartrackingsystem[.]net on October 2, 2018, but do not see a TLS certificate registered. This absence of a TLS certificate does not indicate that there is no certificate, as DomainTools shows a certificate for this domain. More likely, this is a gap in our coverage for certificate registrations for that time period.

Figure 12: Reference showing the domain registration date for virtualwebdata[.]com domain. (Source: Recorded Future)

We see the registration of virtualwebdata[.]com on April 22, 2019, but do not see a TLS certificate registered.

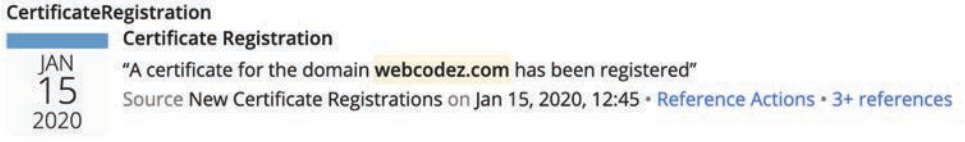


Figure 13: Reference showing the certificate registration date for webcodez[.]com domain. (Source: Recorded Future)

We see the registration of webcodez[.]com on January 15, 2020, but do not see a TLS certificate registered. This is one of the most recent registrations we see from this set of domains.

These delays between domain registration and certification registration suggest that the actor may have parked these domains for future use. As a result, we suggest the addition of ATT&CK sub-technique, T1583.001 Acquire Infrastructure: Domains, to the UNC2452 actor.

Three of the IP addresses associated with the second-stage domains in the DomainTools report were previously seen in Recorded Future. IP addresses 13[.]57[.]184[.]217 and 198[.]12[.]75[.]112 were previously reported on abuseipdb.com on April 6, 2018 and March 19, 2020, respectively. IP address 3[.]16[.]81[.]254 was first seen on a public Pastebin post on January 20, 2019.

Figure 14: Reference showing mention of IP address 13[.]57[.]184[.]217 on AbuseIP Database on April 6, 2018. (Source: Recorded Future)

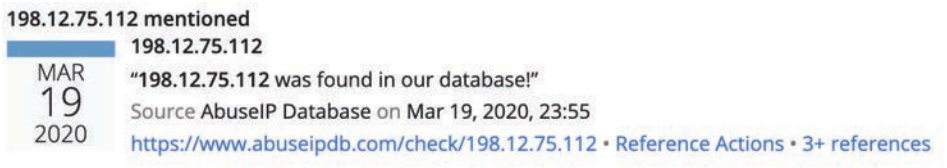


Figure 15: Reference showing mention of IP address 198[.]12[.]75[.]112 on AbuseIP Database on March 19, 2020. (Source: Recorded Future)

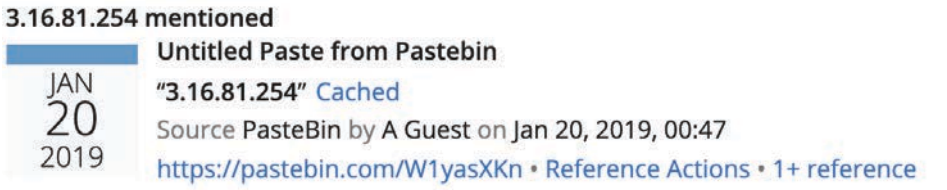


Figure 16: Reference showing mention of IP address 3[.]16[.]81[.]254 on PasteBin on January 20, 2019. (Source: Recorded Future)

45[.]141[.]152[.]18 appears in multiple scans on the site Urlscan.io. Additionally, this IP address appeared on the Recorded Future historic threat list, Recent Hosts of DDNS Names, observed July 19, 2020.

Possibility of Multiple Actors

Microsoft has also published indicators for a second malware which has been discovered to affect the SolarWinds Orion product. It is undetermined whether this malware is associated with the Solorigate backdoor or represents an additional threat actor. As per the Appendix section on the Microsoft blog:

> *"In an interesting turn of events, the investigation of the whole SolarWinds compromise led to the discovery of an additional malware that also affects the SolarWinds Orion product but has been determined to be likely unrelated to this compromise and used by a different threat actor. The malware consists of a small persistence backdoor in the form of a DLL file named App_Web_logoimagehandler.ashx.b6031896.dll, which is programmed to allow remote code execution through SolarWinds web application server when installed in the folder "inetpub\SolarWinds\bin\". Unlike Solorigate, this malicious DLL does not have a digital signature, which suggests that this may be unrelated to the supply chain compromise."*

Microsoft, GuidePoint, and Palo Alto Networks have dubbed this second malware, a .NET webshell, SUPERNOVA. SUPERNOVA is thought to load CosmicGale, a malicious Powershell script. Microsoft advises that if SUPERNOVA is detected on SolarWinds installations, it should be treated as a separate infection. While far from conclusive, this additional malware raises the possibility of multiple actors within the same environment. Multiple actors on the same system, knowingly or unknowingly, are not novel. For example, evidence of both APT28 and APT29 were found on Democratic National Committee servers breached in 2016. Additionally, a file leaked from the ShadowBrokers releases showed 45 file signatures that could be used to scan for infection from other actors, some not publicly known at the time. Still, this adds to the argument that we are far from decisive attribution.

Conclusions

At the Virus Bulletin 2018 conference, security researcher Juan Andres Guerrero-Saade stated, "Currently, our understanding is stated in binary terms: 'is the actor sophisticated or not?'" As evidenced by the plethora of media commentary around this new campaign, not much has changed. We have attempted to add more color to the current picture of attribution, as well as attribution in general.

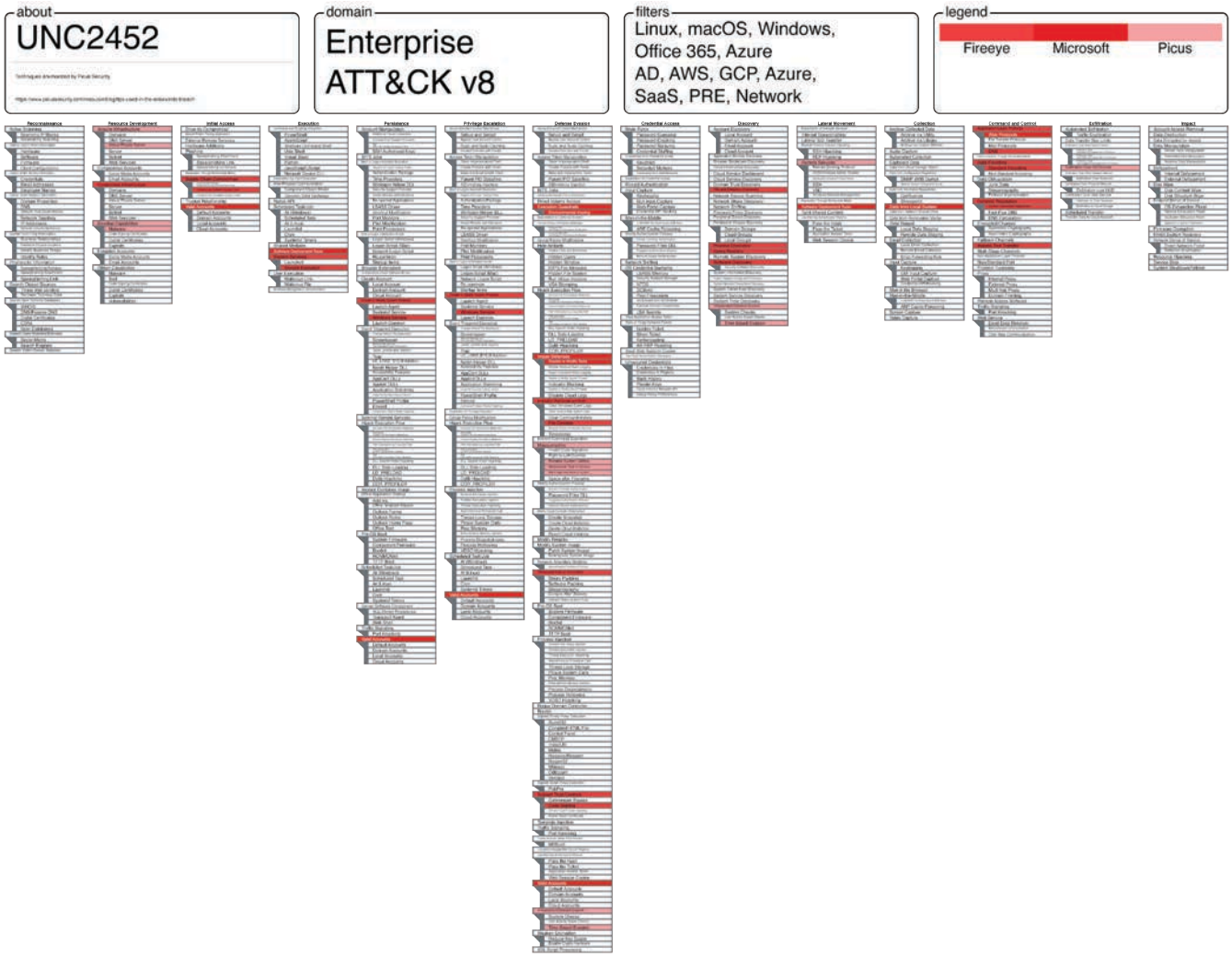
Based on our analysis, we believe the actor behind this campaign is exceptionally focused and patient, even when compared with other state-sponsored campaigns; demonstrates an intricate knowledge of modern information technology practices, architecture, and supply chains; is experienced in a wide variety of attacker techniques; and is very familiar with security researcher techniques and approaches. We don't have a full picture of the details of this intrusion due a variety of factors, including at least partially, balkanized data collection among a variety of security vendors and providers.

The actor behind the SolarWinds breach appears to be selective of targets, both in choosing particular organizations to pursue and purposefully excluding organizations. Careful selection denotes a set of requirements for targeting rather than targets of opportunity commonly seen in cybercrime incidents. Still, this curated targeting evidently included FireEye, a curious choice for a cautious actor. Targeting a company specializing in cybersecurity demonstrates a remarkable audacity, but has been previously seen from both Russian-affiliated actors (NotPetya) and Chinese-affiliated actors (CCleaner). We can conclude this actor either weighed requirements against high risk and believed FireEye was so critical a target as to risk an entire operation, or the actor believed their expertise was such that discovery would not destroy their entire operation. Alternatively, the actor may have been driven by a penchant for revenge: some have speculated part of the motivation behind targeting the Hilary Clinton Presidential Campaign in 2016 was due to her approaches while Secretary of State. Either way, the boldness speaks to the character of the actor, as well as escalates the importance of the companies they excluded. Logically, if they believed discovery was at least a moderate possibility, the actor likely excluded certain organizations from targeting to expand the time until the exposure.

Our analysis of UNC2452 shows no conclusive attribution, however that was not our exclusive intent. Incident responses and investigations are ongoing at dozens of organizations, with hundreds of others assessing impact. The leading theory of a single, known actor, speculated to be the Russian intelligence services or, possibly, a Chinese actor should continue to be assessed. However, we conclude the particular nation behind this campaign is irrelevant for the purposes of tactical defensive actions. Any single actor hypothesis would inevitably be well-funded and state-affiliated, based on the operational time spent prior to breach and the target set involved. Undoubtedly, there will be further information released in coming days and weeks, as the full scope of the campaign comes into focus. Tactically, Recorded Future suggests following the advice provided by security vendors for securing your networks and best practices for conducting investigations. Strategically, we suggest clues be added to public, annotated ATT&CK matrixes of known techniques. In this way, defenders can identify organizational gaps and prioritize improvements based on their level of impact, better assessing risk to the organization at large.

Appendix

MITRE ATT&CK Analysis



Appendix Figure 1: Visualization of compiled UNC2452 techniques, generated on ATT&CK Navigator

We conducted an analysis of UNC2452's known techniques on MITRE ATT&CK Enterprise version 8. UNC2452, as disclosed by FireEye thus far, demonstrates 25 techniques, and 14 sub-techniques under MITRE ATT&CK. (Note: we compared techniques with those enumerated by the original FireEye report on UNC2452, as well as one put together by Picus Security.) We then mapped out UNC2452 technique overlaps with APT29 and APT41. Picus Security adds to certain techniques to their analysis for UNC2452, including:

- T1021 Remote Services
- T1036.003 Masquerade: Rename System Utilities
- T1036.004 Masquerade Task or Service
- T1036.05 Masquerade: Match Legitimate Name or Location
- T1041 Exfiltration over C2 channel
- T1078 Valid Accounts (also seen in Microsoft report)
- T1497.003 Virtualization/Sandbox Evasion: Time Based Evasion
- T1583.003 Acquire Infrastructure: Virtual Private Servers
- T1587.001 Develop Capabilities: Malware

UNC2452 has six techniques overlapped with APT29, and 11 techniques overlapped with APT41. Nine techniques are novel and not seen in either actor's known previous incidents.

Technique Overlaps with APT29

Appendix Figure 2: MITRE ATT&CK mapping of UNC2452 [shown in red] and APT29 [shown in yellow]. Overlapping techniques are shown in orange.

Based on the FireEye report on UNC2452, we track five techniques that overlap with APT29:

Resource Development

- T1583 Acquire Infrastructure (T1583.003 Private Web Server for UNC2452, T1583.006 Web Server)
- T1587 Develop capabilities, though different sub-techniques (Malware T1587.001 for UNC2452, Digital Certificates T1587.003 for APT29)

Initial Access

- T1078 Valid accounts (Domain accounts T1078.002 for APT29)

Execution

- T1569 System Services

Persistence

- T1078 Valid accounts (Domain accounts T1078.002 for APT29)

Privilege Escalation
- T1078 Valid accounts (Domain accounts T1078.002 for APT29)

Defensive Evasion
- T1070 Indicator Removal on Host (File Deletion T1070.004)
- T1078 Valid accounts (Domain accounts T1078.002 for APT29)
- T1027 Obfuscated Files or Information

While this is not conclusive, it can be significant. Techniques shown in APT29 yet not appearing in UNC2452 tracking may be areas for further discovery by defenders. Alternately, these techniques may have not been applied toward this campaign. Conversely, techniques novel to UNC2452 yet not appearing in APT29 may demonstrate newly deployed capabilities. Lack of overlay may open the possibility that UNC2452 is not related to APT29, however this is far from conclusive. Either way, if UNC2452 is ultimately attributed to APT29, this would indicate substantial investment in structure and capabilities.

Differences in UNC2452 and APT29 Techniques

Certain techniques used by UNC2452 have not been observed amongst known techniques for APT29. Rather than disprove association, these could indicate substantial expansion of techniques. If UNC2452 is ultimately synonymized with APT29, we can conclude extensive resources to support such technique expansion:

Initial Access
- T1195 Supply Chain Compromise, Sub-technique T1195.002 Compromise Software Supply Chain

Persistence
- T1543 Create of Modify System Process, Sub-technique T1543.002 Windows Service

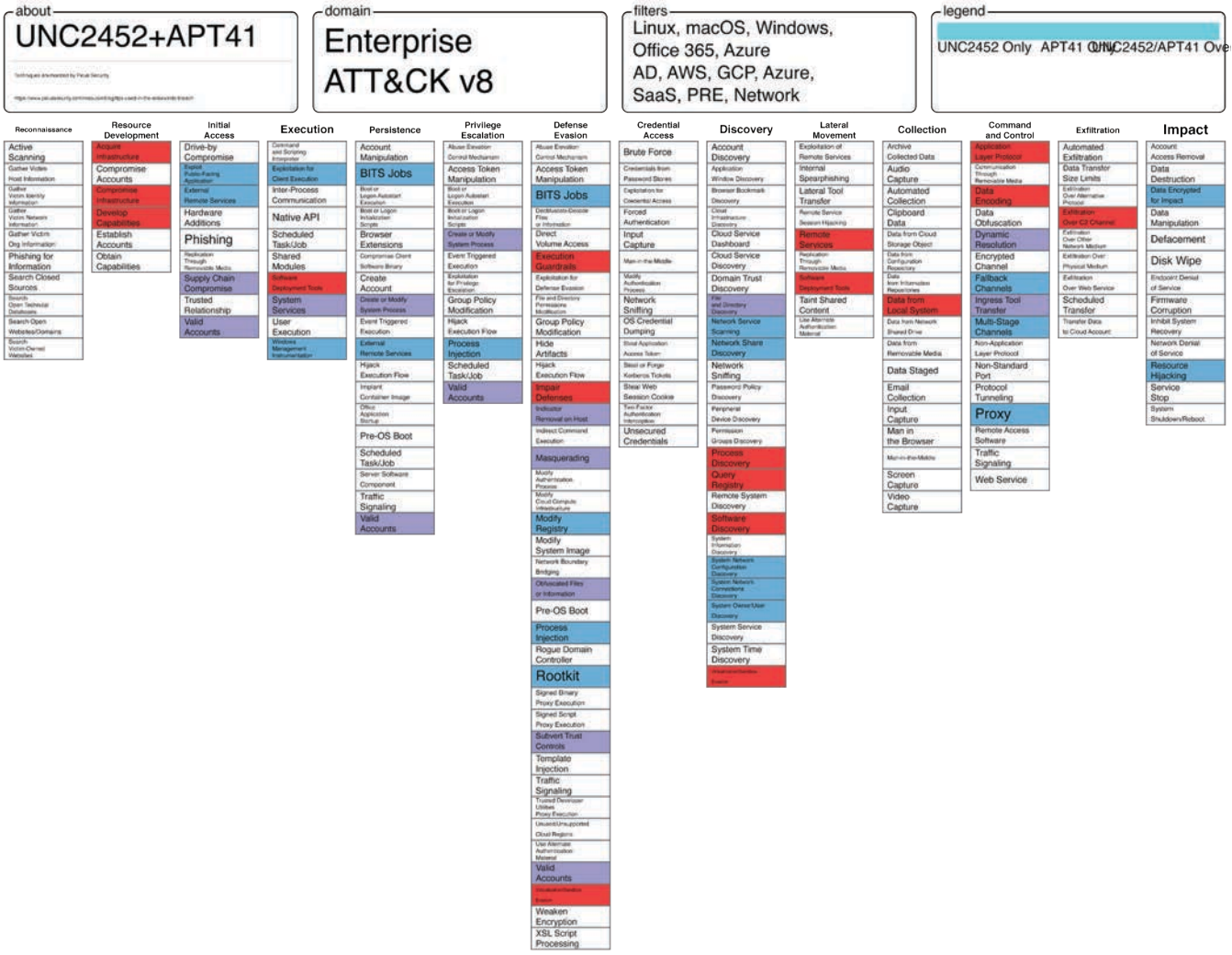
Privilege Escalation
- T1543 Create of Modify System Process, Sub-technique T1543.002 Windows Service

Defensive Evasion
- T1036 Masquerading Sub-techniques T1036.004 Masquerade Task or Service, T1036.05 Match Legitimate Name or Location, T1036.003 Rename System Utilities
- T1553 Subvert Trust Controls, Sub-technique T1553.002 Code Signing
- T1497 Virtualization/Sandbox Evasion, Sub-technique T1497.003 Time Based Evasion

Lateral Movement
- T1021 Remote Services

Command and Control
- T1071 Application Layer Protocol, Sub-technique T1071.001 Web Protocols
- T1568 Dynamic Resolution, T1568.002 Domain Generation Algorithms

UNC2452 Technique Overlaps with APT41



Appendix Figure 3: Visualization of ATT&CK technique comparison between UNC2452 and APT41

Some sources have posited the possibility of threat actors other than APT29 being behind the breach. One possibility which is frequently mentioned is APT41, which is attributed to China according to the September 2020 U.S. Department of Justice indictments of seven defendants, and crosses between state-associated espionage and cybercrime. We identified eight technique overlaps between APT41 and UNC2452:

Initial Access

- T1195 Supply Chain Compromise, Sub-technique T1195.002 Compromise Software Supply Chain
- T1078 Valid Accounts

Execution

- T1569 System Services, Sub-technique T1569.002 Service Execution

Persistence

- T1543 Create or Modify System Processes, Sub-technique T1543.003 Windows Service
- T1078 Valid accounts

Privilege Escalation

- T1543 Create or Modify System Processes, Sub-technique T1543.003 Windows Service
- T1078 Valid accounts

Defensive Evasion
- T1070 Indicator Removal on Host, Sub-technique T1070.004 File Deletion
- T1036 Masquerading Sub-techniques T1036.05 Match Legitimate Name or Location
- T1553 Subvert Trust Controls, Sub-technique T1553.002 Code Signing
- T1078 Valid accounts

Command and Control
- T1568 Dynamic Resolution, T1568.002 Domain Generation Algorithms

Other Actors

Other actors have been posited as candidates for this campaign. Winnti Group has been suggested as a possible candidate actor, given similar DGA patterns seen in 2019 from CCleaner supply chain attacks. Some further analysis is necessary, as the MITRE ATT&CK group for Winnti has only three ATT&CK techniques associated with it:

- T1057, Process Discovery, Winnti Group looked for a specific process running on infected servers
- T1014, Rootkit , Winnti Group used a rootkit to modify typical server functionality
- T1553.002, Subvert Trust Controls: Code Signing, Winnti Group used stolen certificates to sign its malware

These techniques do correspond with techniques leveraged in this campaign, especially the leveraging of a trusted supply chain, however the current campaign is far more expansive, both in terms of technical development and the scope of victims.

Novel Techniques for UNC2452

A subset of techniques in UNC2452 are not seen in known techniques for APT29 nor APT41. Additionally, these techniques are not documented for Winnti either, however this is at least partially attributed to the incomplete MITRE ATT&CK group for this actor:

Execution
- T1072 Software Deployment Tools

Defensive Evasion
- T1036 Masquerading, Sub-techniques T1036.004 Masquerade Task or Service, T1036.003 Rename System Utilities
- T1497 Virtualization/Sandbox Evasion, Sub-technique T1497.003 Time Based Evasion

Discovery
- T1057 Process Discovery
- T1012 Query Registry
- T1480.001 Execution Guardrails: Environmental Keying
- T1497 Virtualization/Sandbox Evasion, Sub-technique T1497.003 Time Based Evasion
- T1562.001 Impair Defense: Disable or Modify Tools

Lateral Movement
- T1021 Remote Services

Command and Control
- T1071 Application Layer Protocol, Sub-technique T1071.001 Web Protocols

Exfiltration
- T1041 Exfiltration of C2 Channel

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.