Threat Intelligence

TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping

April 10, 2019

Mandiant

Written by: Steve Miller, Nathan Brubaker, Daniel Kapellmann Zafra, Dan Caban

Overview

FireEye can now confirm that we have uncovered and are responding to **an additional intrusion by the attacker behind TRITON at a different critical infrastructure facility**.

In December 2017, FireEye publicly released our first analysis on the TRITON attack where malicious actors used the TRITON custom attack framework to manipulate industrial safety systems at a critical infrastructure facility and inadvertently caused a process shutdown. In subsequent research we examined how the attackers may have gained access to critical components needed to build the TRITON attack framework. In our most recent analysis, we attributed the intrusion activity that led to the deployment of TRITON to a Russian government-owned technical research institute in Moscow.

The TRITON intrusion is shrouded in mystery. There has been some public discussion surrounding the TRITON framework and its impact at the target site, yet little to no information has been shared on the tactics, techniques, and procedures (TTPs) related to the intrusion lifecycle, or how the attack made it deep enough to impact the industrial processes. The TRITON framework itself and the intrusion tools the actor used were built and deployed by humans, all of whom had observable human strategies, preferences, and conventions for the custom tooling of the intrusion operation. It is our goal to discuss these adversary methods and highlight exactly how the developer(s)

In this report we continue our research of the actor's operations with a specific focus on a selection of custom information technology (IT) tools and tactics the threat actor leveraged during the early stages of the targeted attack lifecycle (Figure 1). The information in this report is derived from multiple TRITON-related incident responses carried out by FireEye Mandiant.

Using the methodologies described in this post, FireEye Mandiant incident responders have uncovered additional intrusion activity from this threat actor – including new custom tool sets – at a second critical infrastructure facility. As such, we strongly encourage industrial control system (ICS) asset owners to leverage the indicators, TTPs, and detections included in this post to improve their defenses and hunt for related activity in their networks.

For IT and operational technology (OT) incident response support, please contact [FireEye Mandiant](). For more in-depth analysis of TRITON and other cyber threats, consider subscribing to [FireEye Cyber Threat Intelligence]().

FireEye's SmartVision technology, which searches for attackers during lateral movement activities by monitoring east-west traffic in IT and OT networks, reduces the risk of an attack reaching sensitive ICS processes. This is particularly relevant for sophisticated ICS-related intrusions as attackers typically move from corporate IT to OT networks through systems that are accessible to both environments, far beyond perimeter defenses.

Contents

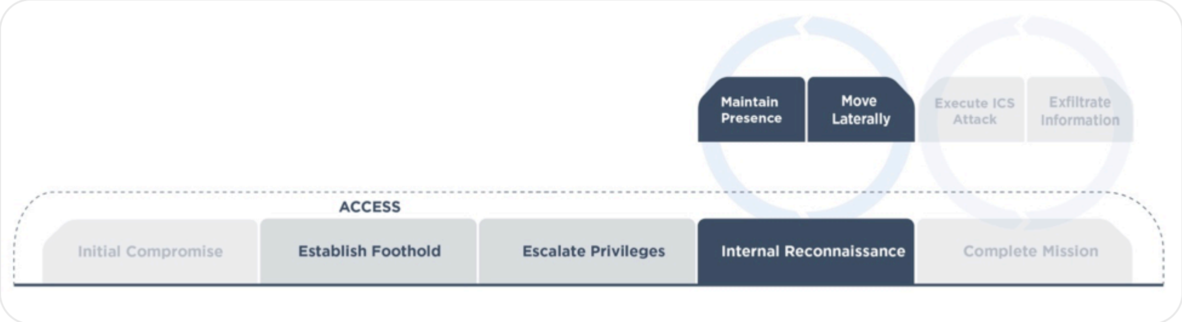

Figure 1: The FireEye targeted attack lifecycle

Actor Leveraged a Variety of Custom and

Throughout the targeted attack lifecycle, the actor leveraged dozens of custom and commodity intrusion tools to gain and maintain access to the target's IT and OT networks. A selection of the custom tools that FireEye Mandiant recovered are listed later in this post in Table 1, and hashes are listed in Table 2 at the end of this post. Discovery rules for and technical analysis of these tools, as well as MITRE ATT&CK JSON raw data, is available in Appendix A, Appendix B, and Appendix C.

TOOL	COMPONENTS	PURPOSE	ATTACK LIFECYCLE STAGE						
			Initial Compromise	Establish Foothold	Escalate Privileges	Internal Reconnaissance	Move Laterally	Maintain Presence	Complete Mission
SecHack	KB77846376.exe KB77846376.exe.x64	Credential harvesting			X	X			
NetExec	NetExec.exe	Remote command execution					X		
	runsvc.exe	NetExec runner							
Cryptcat-based backdoor	cryptcat.exe cryptsvc.exe svchostpla.exe	Backdoor		X					
	compattelprerunner.exe	C&C domain name generator							
	ProgramDataUpdater.xml	Scheduled task file (persistence mechanism)							
PLINK-based backdoor	napupdatedb.exe	Backdoor		X				X	
Bitvise-based backdoor	alg.exe userinit.exe csrss.exe	Backdoor					X	X	
	tquery.dll txflog.dll cryptopp.dll DEFAULT DEFAULT.BAK	Backdoor components							
OpenSSH-based backdoor	spl32.exe WinSAT.exe csrss.exe	Backdoor					X	X	
	clusapi.dll PolicMan.dll verifier2.dll misc.mof setup.ini	Backdoor components							
WebShell	logoff.aspx	Modified legitimate Outlook Web Access Component				X		X	
	flogon.js	Modified legitimate Outlook Web Access Component							
	ftpexts.tlb	Output file containing credentials harvested by logoff.aspx							

Figure 2: Selection of custom tools used by the actor

The actor's custom tools frequently mirrored the functionality of commodity tools and appear to be developed with a focus on anti-virus evasion. The group often leveraged custom tools when they appeared to be struggling with anti-virus detection or were at a critical phase in the intrusion (e.g., they switched to custom backdoors in IT and OT DMZ right before gaining access to the engineering workstation). In some instances, the actor leveraged custom and commodity tools for

SecHack (custom) for credential harvesting; both tools provide a very similar output (Figure 2).

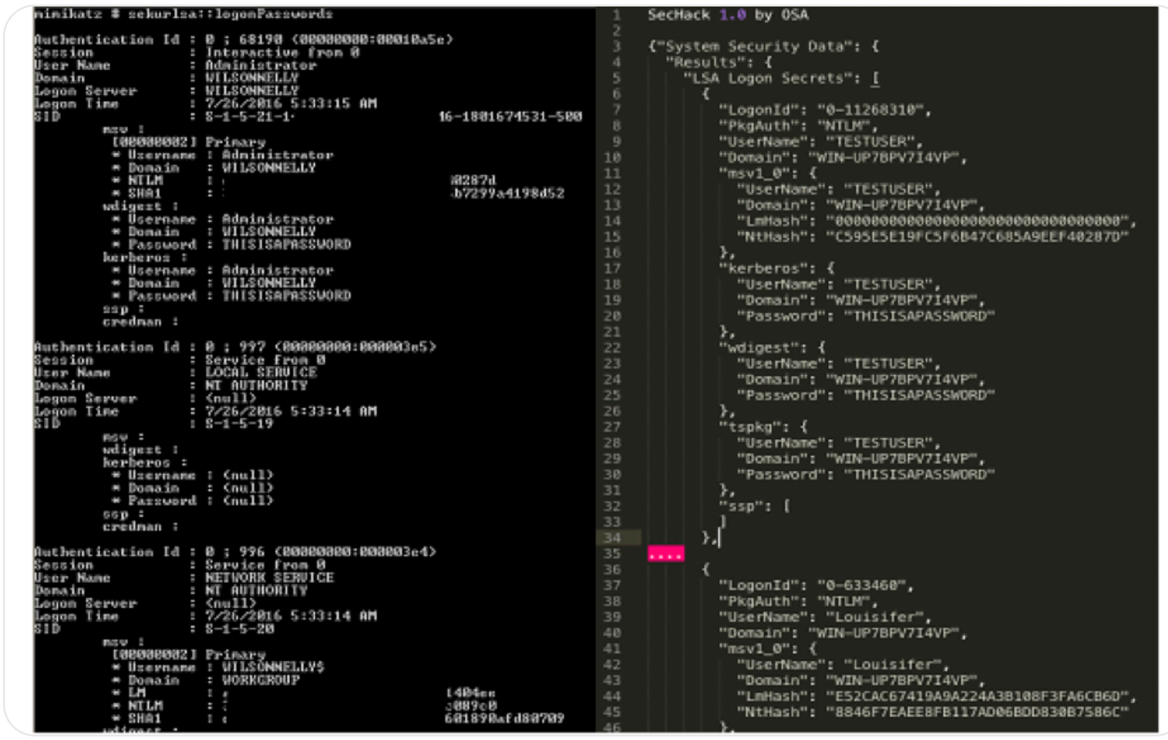

Figure 3: Default outputs for Mimikatz (left) and SecHack (right)

Tools and TTPs Indicate a Deep Interest in Ensuring Prolonged and Persistent Access to the Target Environment

The targeted attack lifecycle of a sophisticated ICS attack is often measured in years. Attackers require a long time to prepare for such an attack in order to learn about the target's industrial processes and build custom tools. These attacks are also often carried out by nation states that may be interested in preparing for contingency operations rather than conducting an immediate attack (e.g., installing malware like TRITON and waiting for the right time to use it). During this time, the attacker must ensure continued access to the target environment or risk losing years of effort and potentially expensive custom ICS malware. This attack was no exception. The actor was present in the target networks for almost a year before gaining access to the Safety Instrumented System (SIS) engineering workstation. Throughout that period, they appeared to prioritize operational security.

After establishing an initial foothold on the corporate network, the TRITON actor focused most of their effort on gaining access to the OT network. They did not exhibit activities commonly associated with espionage, such as using key loggers and screenshot grabbers, browsing files, and/or exfiltrating large amounts of information. Most of the attack tools they used were focused on network reconnaissance, lateral movement, and maintaining presence in the target environment.

The actor used multiple techniques to hide their activities, cover their tracks, and deter forensic examination of their tools and activities.

- They renamed their files to make them look like legitimate files, for example, KB77846376.exe, named after Microsoft update files.

PsExec/WinRM.

- When planting webshells on the Outlook Exchange servers, they modified already existing legitimate flogon.js and logoff.aspx files.
- They relied on encrypted SSH-based tunnels to transfer tools and for remote command/program execution.
- They used multiple staging folders and opted to use directories that were used infrequently by legitimate users or processes.
- They routinely deleted dropped attack tools, execution logs, files staged for exfiltration, and other files after they were finished with them.
- They renamed their tools' filenames in the staging folder so that it would not be possible to identify the malware's purpose, even after it was deleted from the disk through the residual artifacts (e.g., ShimCache entries or WMI Recently Used Apps).
- They used timestomping to modify the $STANDARD_INFORMATION attribute of the attack tools.

Once the actor gained access to the targeted SIS controllers, they appeared to focus solely on maintaining access while attempting to successfully deploy TRITON. This involved strategically limiting their activities to mitigate the risk of being discovered.

- The actor gained a foothold on the distributed control system (DCS) but did not leverage that access to learn about plant operations, exfiltrate sensitive information, tamper with the DCS controllers, or manipulate the process.
- They then gained access to an SIS engineering workstation. From this point forward, they focused most of their effort on delivering and refining a backdoor payload using the TRITON attack framework.
- They attempted to reduce the chance of being observed during higher-risk activities by interacting with target controllers during off-hour times. This would ensure fewer workers were on site to react to potential alarms caused by controller manipulation.
- They renamed their files to make them look like legitimate files, for example, trilog.exe, named after a legitimate Schneider Electric application.

Operational Since At Least 2014

Based on analysis of the actor’s custom intrusion tools, the group has been operating since as early as 2014. It is worth noting that FireEye had never before encountered any of the actor's custom tools, despite the fact that many of them date to several years before the initial compromise. This fact and the actor's demonstrated interest in operational security suggests there may be other target environments – beyond the second intrusion announced in this blog post – where the actor was or still is present.

- A sample of a Cryptcat-based backdoor used to establish the initial foothold was recovered during the investigation; the sample was compiled and uploaded to a malware testing environment by the actor in 2014.
- Cryptcat- and PLINK-based backdoors were scheduled to execute daily starting from April 28, 2014, using ProgramDataUpdater and NetworkAccessProtectionUpdateDB tasks. This date is unrelated to the observed intrusion timeline and may indicate the date the threat actors first created these persistence mechanisms.
- NetExec.exe, a custom lateral movement and remote command execution tool, is self-titled "NetExec 2014 by OSA."
- SecHack.exe "by OSA," a custom credential harvesting and reconnaissance tool, was compiled on Oct. 23, 2014.
- The attackers used a pirated version of Wii.exe, a public file indexing tool that came with a license from 2010 and has not been updated since 2014.

ICS Asset Owners Should Prioritize Detection and Defense Across Windows Systems in Both IT and OT

Most sophisticated ICS attacks leveraged Windows, Linux, and other traditionally "IT" systems (located in either IT or OT networks) as a conduit to the ultimate target. Some examples include leveraging computers to gain access to targeted PLCs (e.g., Stuxnet), interacting directly with internet-connected human machine interfaces (HMIs) (e.g., BlackEnergy), and gaining remote access to an engineering station to manipulate a remote terminal unit (RTU) (e.g., INDUSTROYER) or infect SIS programmable logic controllers (PLC) (e.g., TRITON).

Defenders who focus on stopping an attacker in these "conduit" systems benefit from a number of key advantages. These advantages will only grow as IT and OT systems continue to converge.

- Attackers commonly leave a broad footprint in IT systems across most if not all the attack lifecycle.
- It is ideal to stop an attacker as early in the attack lifecycle as possible (aka "left of boom"). Once an attacker reaches the targeted ICS, the potential of a negative outcome and its severity for the target increase dramatically.
- There are many mature security tools, services, and other capabilities already available that can be leveraged to defend and hunt in "conduit" systems.

Leveraging Known Tools and TTPs To Hunt For the TRITON Actor

Historic activity associated with this actor demonstrates a strong development capability for custom tooling. The developer(s) behind these toolsets leaned heavily on existing software frameworks and modified them to best serve the intrusion operations. The developer(s) had preferences regarding the ports, protocols, persistence mechanisms, and other aspects of how the malware operated.

While the preferences of the development team supporting this activity will likely shift and change over time, learning about them is still useful to identify whether their TTPs are applicable to other malware developers and threat actors. Additionally, the actor possibly gained a foothold on other target networks—beyond the two intrusions discussed in this post – using similar strategies. In such cases, retrospective hunting would help defenders identify and remediate malicious activity.

Based on the examination of developer(s) preferences and abstracted adversary methodologies, it is possible to build broader visibility of the TTPs using detection and hunting rules of various fidelity and threat density. The compilation of these rules makes it possible to identify and classify potentially malicious samples while building new "haystacks" in which to hunt for adversary activity.

The TTPs we extracted from this actor's activities are not necessarily exclusive, nor are they necessarily malicious in every circumstance. However, the TTP profile built by FireEye can be used to search for patterns of evil in subsets of network and endpoint activity. Not only can these TTPs be used to find evidence of intrusions, but identification of activity that has strong overlaps with the actor's favored techniques can lead to stronger assessments of actor association, further bolstering incident response efforts.

The following table provides insights into notable methodologies surrounding the use of custom tools and tips for identifying evidence of this and related activity. Adversary methodologies are also expressed in terms of the MITRE ATT&CK framework (see Appendix C for MITRE ATT&CK JSON raw data).

Adversary Methodology	**Discovery Tips**
Persistence by Scheduled Tasks by XML trigger ATT&CK: T1053	Look for new and anomalous Scheduled Tasks XML unsigned .exe files.

Persistence by IFEO injection [ATT&CK: T1183](#)	Look for modifications and new entries referencing key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\\ NT\CurrentVersion\Image File Execution Options.
Command and control (C2) established using hard-coded DNS servers	Look for PEs executions with run DNS lookups to 8. applicable to sandbox and other malware processin
C2 using favored C2ports [ATT&CK: T1043](#) [ATT&CK: T1065](#)	Look for outbound connections with port-protocol and uncommon ports such as 443, 4444, 8531, and
C2 using favored Virtual Private Server (VPS) infrastructure [ATT&CK: T1329](#)	Look for inbound and outbound connections from a ranges, especially from international VPS providers Limited (uk2.net).
C2 domains with hyphen	Look for newly observed 2LD and 3LD domains tha
C&C using dynamic DNS domains from afraid.org [ATT&CK: T1311](#)	Look for newly observed dynamic DNS domains ow afraid.org.
C2 domains registered with vfemail.net email addresses	Look for newly observed domains or DNS resolutior registrant email information containing vfemail.net

Tunneled RDP using PLINK [ATT&CK: T1076]()	Look for the presence of PLINK and non-standard F logs, firewall logs, and registry keys as described in "[Bypassing Network Restrictions Through RDP Tunn]() Find internal RDP pivoting by looking for bitmap cac accounts that should not be accessing sensitive sys bitmap cache files such as bcache22.bmc under de administrator accounts or any account not expecte internal RDP accesses to sensitive systems in a prot zone, especially in the DMZ or DCS areas like HMIs workstations.
C2 using hard-coded SSH private keys	Look for PEs with hard-coded OpenSSH private key
Use of direct RDP [ATT&CK: T1076]()	Look for inbound RDP connections with default hos standard or unexpected locale IDs, or other metada [blog post on baselining RDP]() activity.
C2 using source systems with default Windows hostnames	Look for default Windows hostnames that fit the str (e.g., WIN-ABCDEFGH1JK) in PE certificates, SSL an RDP handshakes.
C2 using SSH	Look for new, unique, or unusual SSH sessions. Log fingerprints would quickly and easily identify an ano result of malware. Look for SSH over non-standard
Compromised VPN accounts [ATT&CK: T1078]()	Look for VPN logon anomalies based on infeasible p account location, IP address, and hostname associ FireEye blog post and free toolset for VPN logon an If you use SMS-based MFA, look for phone numbers country where your employees operate.
Malware masquerading as Microsoft Corporation	Look for PEs with mismatched PE metadata such as strings and also "Microsoft Corporation" in the met unsigned "Microsoft Corporation" binaries in the gr directories.
Use of customized Bitvise binaries	Look for PEs with Bitvise PDB path strings such as c

Use of customized OpenSSH binaries	Look for PEs with content "Microsoft openSSH clien
Use of customized Cryptcat but with default password	Look for PEs that drop Cryptcat binaries or contain such as the default password "metallica."
Timestomping via PowerShell ATT&CK: T1099	Look for timestomping command strings such as ".(PowerShell scripts or in PowerShell command-line e NTFS creation time prior to PE compile time.
Deployment of binaries with debug information from developer workstations with Visual Studio 2010	Look for PEs with PDB paths containing default or g • \Users\user\Documents\Visual Studio 2010\ • \Documents\Visual Studio 2010\.
Use of Thinstall for packaging malware	Look for PE with content "thinstall\modules\boot_lo Thinstall binaries that have created virtualized files i SYSTEM user "C:\Windows\SysWOW64\config\systemprofile\AppD
Use of favored directories for operating, staging and executing files	Look for new, unexpected, or otherwise anomalous directories: • C:\Windows\system32\inetsrv\ • C:\Windows\temp\ • C:\Windows\SysWOW64\wbem • C:\Windows\SysWOW64\drivers • C:\Windows\SysWOW64 • C:\Windows\system32\wbem\ • C:\Windows\system32\drivers\ • C:\Windows\system32\ • C:\Windows\ • C:\Users\Public\Libraries\ • C:\Users\administrator\appdata\local\temp\ • C:\ssh\

	• C:\perflogs\admin\servermanager\ • C:\perflogs\admin\ • C:\perflogs\ • C:\cpqsystem\ • C:\hp\hpdiags\ • C:\hp\bin\log\

Table 1: TRITON actor methodology and discovery strategies

Outlook

There is often a singular focus from the security community on ICS malware largely due to its novel nature and the fact that there are very few examples found in the wild. While this attention is useful for a variety of reasons, we argue that defenders and incident responders should focus more attention on so-called "conduit" systems when trying to identify or stop ICS-focused intrusions.

In an attempt to raise community awareness surrounding this actor's capabilities and activities between 2014 and 2017—an effort compounded in importance by our discovery of the threat actor in a second critical infrastructure facility—we have shared a sampling of what we know about the group's TTPs and custom tooling. We encourage ICS asset owners to leverage the detection rules and other information included in this report to hunt for related activity as we believe there is a good chance the threat actor was or is present in other target networks.

For IT and OT incident response support, please contact FireEye Mandiant. For more in-depth analysis of TRITON and other cyber threats, consider subscribing to FireEye Cyber Threat Intelligence.

FireEye's SmartVision technology, which searches for attackers during lateral movement activities by monitoring east-west traffic in IT and OT networks, reduces the risk of an attack reaching sensitive ICS processes. This is particularly relevant for sophisticated ICS-related intrusions as attackers typically move from corporate IT to OT networks through systems that were accessible to both environments, far beyond perimeter defenses.

Appendices

- Appendix A: Discovery Rules
- Appendix B: Technical Analysis of Custom Attack Tools
- Appendix C: MITRE ATT&CK JSON Raw Data

Related articles

Threat Intelligence
Hybrid Russian Espionage and Influence Campaign Aims to Compromise Ukrainian Military Recruits and Deliver Anti-Mobilization Narratives
By Google Threat Intelligence Group • 10-minute read

Threat Intelligence
Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575)
By Mandiant • 19-minute read

Threat Intelligence
How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends
By Mandiant • 10-minute read

Threat Intelligence
capa Explorer Web: A Web-Based Tool for Program Capability Analysis
By Mandiant • 6-minute read

Follow us

Google Cloud Google Cloud Products Privacy Terms Help English