# TEMP.Veles, XENOTIME, Group G0088 | MITRE ATT&CK®

Archived: 2026-04-02 10:49:47 UTC

Enterprise T1583 .003 Acquire Infrastructure: Virtual Private Server

During the C0032 campaign, TEMP.Veles used Virtual Private Server (VPS) infrastructure.[1]

Enterprise T1595 Active Scanning

In the Triton Safety Instrumented System Attack, TEMP.Veles engaged in network reconnaissance against targets of interest.[2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

In the Triton Safety Instrumented System Attack, TEMP.Veles used a publicly available PowerShell-based tool, WMImplant.[2]

During the C0032 campaign, TEMP.Veles used PowerShell to perform timestomping.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

During the C0032 campaign, TEMP.Veles used staging folders that are infrequently used by legitimate users or processes to store data for exfiltration and tool deployment.[1]

Enterprise T1587 .001 Develop Capabilities: Malware

In the Triton Safety Instrumented System Attack, TEMP.Veles developed, prior to the attack, malware capabilities that would require access to specific and specialized hardware and software.[7]

Enterprise T1573 Encrypted Channel

In the Triton Safety Instrumented System Attack, TEMP.Veles used cryptcat binaries to encrypt their traffic.[2]

Enterprise T1546 .012 Event Triggered Execution: Image File Execution Options Injection

During the C0032 campaign, TEMP.Veles modified and added entries within `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options` to maintain persistence.[1]

Enterprise T1133 External Remote Services

During the C0032 campaign, TEMP.Veles used VPN access to persist in the victim environment.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

During the C0032 campaign, TEMP.Veles routinely deleted tools, logs, and other files after they were finished with them.[1]

.006 Indicator Removal: Timestomp

During the C0032 campaign, TEMP.Veles used timestomping to modify the `$STANDARD_INFORMATION` attribute on tools.[1]

Enterprise T1056 .003 Input Capture: Web Portal Capture

In the Triton Safety Instrumented System Attack, TEMP.Veles captured credentials as they were being changed by redirecting text-based login codes to websites they controlled.[6]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

In the Triton Safety Instrumented System Attack, TEMP.Veles renamed files to look like legitimate files, such as Windows update files or Schneider Electric application files.

During the C0032 campaign, TEMP.Veles renamed files to look like legitimate files, such as Windows update files or Schneider Electric application files.[1]

Enterprise T1571 Non-Standard Port

During the C0032 campaign, TEMP.Veles used port-protocol mismatches on ports such as 443, 4444, 8531, and 50501 during C2.[1]

Enterprise T1027 .005 Obfuscated Files or Information: Indicator Removal from Tools

In the Triton Safety Instrumented System Attack, TEMP.Veles modified files based on the open-source project cryptcat in an apparent attempt to decrease anti-virus detection rates.[2]

Enterprise T1588 .002 Obtain Capabilities: Tool

In the Triton Safety Instrumented System Attack, TEMP.Veles used tools such as Mimikatz and other open-source software.[2]

During the C0032 campaign, TEMP.Veles obtained and used tools such as Mimikatz and PsExec.[1]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

In the Triton Safety Instrumented System Attack, TEMP.Veles used Mimikatz.[8]

During the C0032 campaign, TEMP.Veles used Mimikatz and a custom tool, SecHack, to harvest credentials.[1]

Enterprise T1572 Protocol Tunneling

During the C0032 campaign, TEMP.Veles used encrypted SSH-based PLINK tunnels to transfer tools and enable RDP connections throughout the environment.[1]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

During the C0032 campaign, TEMP.Veles utilized RDP throughout an operation.[1]

.004 Remote Services: SSH

During the C0032 campaign, TEMP.Veles relied on encrypted SSH-based tunnels to transfer tools and for remote command/program execution.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

In the Triton Safety Instrumented System Attack, TEMP.Veles installed scheduled tasks defined in XML files.[2]

During the C0032 campaign, TEMP.Veles used scheduled task XML triggers.[1]

Enterprise T1505 .003 Server Software Component: Web Shell

During the C0032 campaign, TEMP.Veles planted Web shells on Outlook Exchange servers.[1]

Enterprise T1078 Valid Accounts

During the C0032 campaign, TEMP.Veles used compromised VPN accounts.[1]

ICS T0830 Adversary-in-the-Middle

In the Triton Safety Instrumented System Attack, TEMP.Veles changed phone numbers tied to certain specific accounts in a designated contact list. They then used the changed phone numbers to redirect network traffic to websites controlled by them, thereby allowing them to capture and use any login codes sent to the devices via text message.[6]

ICS T0807 Command-Line Interface

In the Triton Safety Instrumented System Attack, TEMP.Veles' tool took one option from the command line, which was a single IP address of the target Triconex device.[7]

ICS T0817 Drive-by Compromise

TEMP.Veles utilizes watering hole websites to target industrial employees. [9]

ICS T0872 Indicator Removal on Host

In the Triton Safety Instrumented System Attack, TEMP.Veles would programmatically return the controller to a normal running state if the Triton malware failed. If the controller could not recover in a defined time window, TEMP.Veles programmatically overwrote their malicious program with invalid data.[7]

ICS T0867 Lateral Tool Transfer

In the Triton Safety Instrumented System Attack, TEMP.Veles made attempts on multiple victim machines to transfer and execute the WMImplant tool.[2]

ICS T0828 Loss of Productivity and Revenue

In the Triton Safety Instrumented System Attack, TEMP.Veles tripped a controller into a failed safe state, which caused an automatic shutdown of the plant, this resulted in a pause of plant operations for more than a week. Thereby impacting industrial processes and halting productivity.[7]

ICS T0843 Program Download

In the Triton Safety Instrumented System Attack, TEMP.Veles downloaded multiple rounds of control logic to the Safety Instrumented System (SIS) controllers through a program append operation.[7]

ICS T0886 Remote Services

In the Triton Safety Instrumented System Attack, TEMP.Veles utilized remote desktop protocol (RDP) jump boxes, poorly configured OT firewalls [6], along with other traditional malware backdoors, to move into the ICS environment.[8][6]

ICS T0853 Scripting

In the Triton Safety Instrumented System Attack, TEMP.Veles used a publicly available PowerShell-based tool, WMImplant.[2]

ICS T0862 Supply Chain Compromise

TEMP.Veles targeted several ICS vendors and manufacturers. [10]

ICS T0855 Unauthorized Command Message

In the Triton Safety Instrumented System Attack, TEMP.Veles leveraged Triton to send unauthorized command messages to the Triconex safety controllers.[8]

ICS T0859 Valid Accounts

In the Triton Safety Instrumented System Attack, TEMP.Veles used valid credentials when laterally moving through RDP jump boxes into the ICS environment.[8]

---