



# Agenda


- Who are we?
- What is a AtomicTestHarness?
- Msiexec
- Service Creates
- Discussion
- Next time on *Atomics On A Friday*



# Who Are We?




Michael Haag  
**Sr. Threat Connoisseur**

 @M\_Haggis




Justin Elze  
**Hacker/CTO @TrustedSec**

 @HackingLZ



Paul Michaud  
**Principal Handler of Shenanigans**

 @Burning\_PM



# ATH - AtomicTestHarnesses

Technique

Variations

Testing GUID

Success/Failure

..
T1003.001_DumpLSASS
T1055.002_PortableExecutableInjection
T1055_ProcessInjection
T1059.001_PowerShell
T1078.003_ValidAccounts
T1112_ModifyRegistry
T1127.001_MSBuild
T1134.001_TokenImpersonation
T1134.002_CreateProcessWithToken
T1134.004_ParentPIDSpooing
T1218.001_CompiledHTMLFile
T1218.005_Mshta
T1218.007_Msiexec
T1218_SignedBinaryProxyExecution
T1543.003_WindowsService
T1574.012_COR_PROFILER

**Testing adversary  
technique variations  
with  
AtomicTestHarnesses**



# CTI and Msiexec

**Max\_Malyutin** @Max\_Ma\_ · Dec 7, 2022

#IcedID (#BokBot) MSI Infection TTPs 🚩

[+] HTML Smuggling (T1027.006)

[+] **Msiexec** - .msi stager (T1218.007)

[+] Rundll32 - .dll loader (T1218.011)

[+] New export func: init, a short version of PluginInit 🔥

#DFIR exec flow:

msi > [RPC Install] &gt; **msiexec** > rundll32

CVE-2021-44077

Exfiltrate Data

exploit

Plink

## Will the Real Msiexec Please Stand Up? Exploit Leads to Data Exfiltration

June 6, 2022

In this multi-day intrusion, we observed a threat actor gain initial access to an organization by exploiting a vulnerability in ManageEngine SupportCenter Plus. The threat actor, discovered files on the server and dumped credentials using a web shell, moved laterally to key servers using Plink and RDP and exfiltrated sensitive information using the web shell and RDP.

The FBI and CISA published an [advisory](#), noting that APT attackers were using [CVE-2021-44077](#) to gain initial access to the networks of organizations of Critical Infrastructure Sectors such as healthcare, financial, electronics and IT consulting industries.

**Max\_Malyutin** @Max\_Ma\_ · Feb 2

#Qakbot Pushing MSI Fake TeamViewer 🚩

Exec flow #DFIR & #TTPs:

MSI > [RPC] > **msiexec** > Rundll32 > [injection target process]

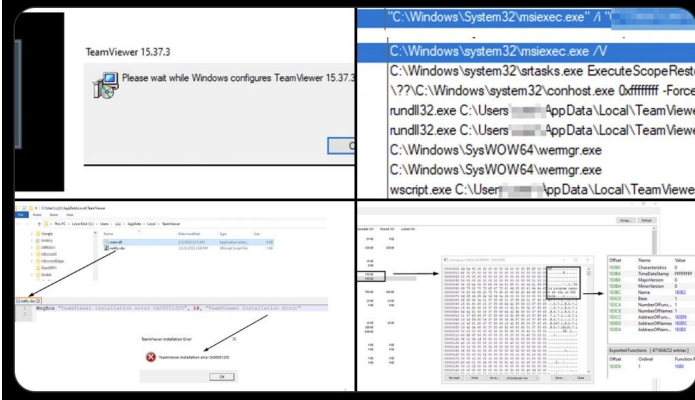
[+] **Msiexec** T1218.007

[+] Rundll32 T1218.011; export func: Updt

[+] Process Injection T1055

[+] Loader internal name: comrepl.dll

H/T @ian\_kenefick 🙏



# ATH and Msiexec

What is a MSI?

System Binary Proxy Execution: Msiexec T1218.007

<https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/msiexec>



# ATH and Service Create

What is a service create?

Create or Modify System Process: Windows Service  
Types:

KernelDriver, FileSystemDriver, Win32**Own**Process,  
Win32**Share**Process

Note the parallels: new-service < — > sc.exe



# CTI Service Create

<https://attack.mitre.org/techniques/T1543/003/>

## Procedure Examples

ID	Name	Description
S0504	Anchor	Anchor can establish persistence by creating a service. <sup>[6]</sup>
S0584	AppleJeus	AppleJeus can install itself as a service. <sup>[7]</sup>
G0073	APT19	An APT19 Port 22 malware variant registers itself as a service. <sup>[8]</sup>
G0022	APT3	APT3 has a tool that creates a new service for persistence. <sup>[9]</sup>
G0050	APT32	APT32 modified Windows Services to ensure PowerShell scripts were loaded on the system. <sup>[10][11][12]</sup>
G0082	APT38	APT38 has installed a new Windows service to establish persistence. <sup>[13]</sup>
G0096	APT41	APT41 modified legitimate Windows services to install malware backdoors. <sup>[14][15]</sup> APT41 created a service named Strike. <sup>[16]</sup>
S0438	Attor	Attor's dispatcher can establish persistence by registering a new service. <sup>[17]</sup>
S0347	AuditCred	AuditCred is installed as a new service on the system. <sup>[18]</sup>
S0239	Bankshot	Bankshot can terminate a specific process by its process id. <sup>[19][20]</sup>
S0127	BBSRAT	BBSRAT can modify service configurations. <sup>[21]</sup>

POSTED: 28 FEB, 2022 | 9 MIN READ | THREAT INTELLIGENCE

 SUBSCRIBE

 FOLLOW  

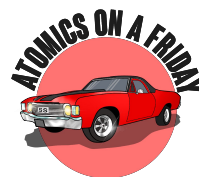
## Daxin: Stealthy Backdoor Designed for Attacks Against Hardened Networks

Espionage tool is the most advanced piece of malware Symantec researchers have seen from China-linked actors.





# DEMO



# Mitigations

## Detection:

- 4104 - Script Block Logging
- 4688 / Sysmon / EDR
- 7045 / 4697 New Service installed
- Track modloads (msi.dll, jscript, vbscript, amsi)

## Prevention

- WDAC + MSI
- WDAC + Driver blocklist
- HVCI
- ASR
- Any AppControl



Thank you

- <https://github.com/redcanaryco/invoke-atomicredteam>
- <https://github.com/redcanaryco/AtomicTestHarnesses>
- <http://atomicredteam.io>
- <https://attack.mitre.org/techniques/T1218/007/>
- Atomics on A Friday Github repo: <https://github.com/Atoms-on-A-Friday>

