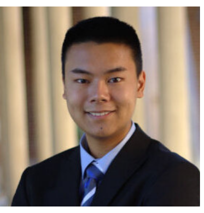
red canary

RESOURCES • BLOG

THREAT INTELLIGENCE



MSIX installer malware delivery on the rise across multiple campaigns

We've seen multiple distinct adversaries leveraging MSIX installers to deliver a variety of malware payloads in recent months.

TONY LAMBERT • TYLER BOHLMANN • CHRISTINA JOHNS • FRANK LEE

Originally published January 12, 2024.
Last modified October 2, 2024.

Starting in July 2023, Red Canary began investigating a series of attacks by adversaries leveraging MSIX files to deliver malware. **MSIX** is a Windows application package installation format that IT teams and developers increasingly use to deliver Windows applications within enterprises.

Threat clusters abusing MSIX installers to deliver malware

Analysis of the intrusions revealed three clusters of activity stretching from July to December 2023.

Cluster 1: FIN7

The first cluster of activity we've observed seems to bear the hallmarks of a financially motivated threat group known as FIN7 that's been active since at least 2015. They've leveraged many malicious tools over the years and represent a significant risk to organizations, in part because FIN7 activity has frequently preceded **ransomware deployment**. We've detected activity within this cluster attempting to install malicious instances of **NetSupport Manager RAT**.

In the detections we've observed within this cluster, the adversary leverages the **MSIX-PackageSupportFramework** tool to create their malicious MSIX files. When the victim opens the MSIX, the `StartingScriptWrapper.ps1` component of the MSIX package support framework launches an embedded **PowerShell** script.

The PowerShell script employs **process injection** to execute **POWERTRASH** and **Carbanak** malware, which in turn deliver **NetSupport Manager RAT** as a follow-on payload. Notably, the NetSupport RAT binaries in these intrusions contain metadata associated with an entity called "Crosstec Corporation" rather than the expected "NetSupport Corporation." Recent **research from Microsoft** corroborates our assessment that FIN7, which Microsoft tracks as **Sangria Tempest**, may be behind these incidents.

Cluster 2: Zloader

The adversary in Cluster 2 uses Advanced Installer—a development utility widely used for building software installation packages—to create MSIX files. These MSIX files leverage the legitimate Advanced Installer binary `AiStub.exe` to execute the malicious payload inside.

The payload is named `Install.exe` and is constructed using compiled Python code. Red Canary's analysis of the Python payloads reveal at least some consistent overlap with **Zloader** (aka BatLoader), including using OpenSSL commands to decrypt components and the use of `GetAdmin.vbs` scripts. The same research from Microsoft (**referenced above**) suggests this cluster also overlaps or aligns with a group Microsoft identifies as Storm-0569.

Cluster 3: FakeBat

Similar to Cluster 2, the adversary in Cluster 3 also uses Advanced Installer to create MSIX files. The Cluster 3 payload is a malicious PowerShell script, which `AiStub.exe` executes via the legitimate component `StartingScriptWrapper.ps1`.

Adversaries in Cluster 3 intrusions have used ArechClient2 or **Redline stealer** in the same chain of activity. The adversary's packages have also delivered a **DLL-sideloading** payload consistent with GHOSTPULSE, as well as using GPG decryption tools and tar to decompress files in a manner consistent with **FakeBat**. FakeBat has also been used in MSIX packages to distribute additional payloads in the past, notably **IcedID**. **Research from Microsoft suggests** this cluster overlaps or aligns with a group they call Storm-1113.

Why should organizations care about this?

Security is a cat-and-mouse game between adversaries and defenders, and the intrusions Red Canary observed and responded to demonstrate that preventative security controls alone are not adequate.

Following an uptick of malware delivered via MSIX, Microsoft disabled the `ms-appinstaller` **protocol** from February 2022 up until August 2022 to address a **vulnerability** that allowed attackers to distribute remote MSIX packages that appear to be from a trusted source. While this mitigated some threats, **other security researchers** noted that legitimate code-signing certificate services could be acquired illicitly from criminal forums, and that MSIX installers could still distribute malware if they were downloaded locally to a victim's system first.

In December 2023, Microsoft again **disabled the protocol** to address increased MSIX use to distribute malware from remote URLs. In this case, Microsoft chose to leave the protocol disabled by default, requiring a configuration change to enable it. As with previous encounters with MSIX files, this disabling solution does not fully eliminate the threat of MSIX files, it merely requires the malicious MSIX files to be intentionally downloaded to disk before execution.

> Preventative security controls alone are not adequate.

Since at least December 2022, adversaries have also abused advertisement solutions such as Google Ads to deliver malware of various types, including MSIX files, posing as legitimate software. Google Ads provide methods for companies to advertise using their product—namely, by putting promoted advertisements ahead of organic results. While Google and other search companies have attempted to curb SEO poisoning and malicious advertising, adversaries have continued to modify their tactics to evade anti-SEO poisoning efforts.

Victims of the malware distributed using these MSIX installers are often prime targets for follow-on activity through persistent access via remote access tools or credential access

What can you do about malicious MSIX installers?

While the increase in abuse of malicious MSIX installers is certainly an emergent trend, the adversaries behind it are still at least partially reliant on fairly well understood tradecraft. Fortunately, we can share a few pseudo-detectors that have helped us catch these and other threats. For prevention, organizations that use application allow-listing solutions such as AppLocker can explore **allowing or denying MSIX execution with AppLocker policies.**

Detection opportunity 1: Launching PowerShell scripts from `windowsapps` directory

This pseudo-detector looks for the execution of PowerShell scripts from the `windowsapps` directory. There are instances where benign PowerShell scripts run from this directory, but analysts can sort out malicious or suspicious activity by investigating follow-on actions and network connections. However, in this case we see the adversary calling `StartingScriptWrapper.ps1` from the `windowsapps` directory to execute their malicious payload script.

```
parent_process_path_includes (‘\\windowsapps\\’)

&&

process == (‘powershell.exe’)

&&

command_includes (‘windowsapps' && '-file ' &&
'.ps1')
```

Detection opportunity 2: NetSupport running from unexpected directory

running outside the `program files` directory, particularly from the `programdata` directory, then it’s worth investigating.

Detection opportunity 3: Abusing PowerShell to disable Defender components

We also observed at least one of these adversaries abusing PowerShell to exclude certain files or processes from Windows Defender scanning. Luckily, this is common tradecraft for which we’ve shared **similar detection ideas** on multiple occasions. The following may unearth this and other threats:

```
process == (‘powershell.exe’)

&&

command_line_includes (‘Set-MpPreference’ || ‘Add-MpPreference’)

&&

command_line_includes (‘ExclusionProcess’ || ’ExclusionPath’)
```

Detection opportunity 4: PowerShell `-encodedcommand` switch

We also observed at least one of these adversaries abusing the shortened `-encoded` PowerShell command switch to encode PowerShell commands. This is another common bit of tradecraft that we’ve discussed many times on the **Red Canary blog**, in the **Threat Detection Report**, and elsewhere. The following should help detect it.

```
process == ('powershell.exe')
```

```
        enco'|| [any variation of the encoded command
        switch])*
```

**Note that PowerShell will recognize anything from the shortened -e to the full `-encodedcommand` and `encode` commands accordingly.*

Detection opportunity 5: MSBuild without commands

In some detections, we observed the Microsoft Build Engine (`msbuild.exe`) making outbound network connections to IPs associated with the ArechClient2 remote access tool. In general, it is suspicious for `msbuild.exe` to execute without a corresponding command line, which is precisely what we observed here. Simply looking for execution of `msbuild.exe` without a corresponding command line and examining surrounding activity for suspicious network connections and child processes could help detect this threat.

In the tables below, you'll find indicators of compromise (IOC) and MITRE mappings for each of the three activity clusters.

CLUSTER 1 INDICATORS OF COMPROMISE

IOC	CONTEXT
grammarly.yesofts[.]com	Typosquatted Grammarly domain
storageplace[.]pro	Resolves to 193.233.22[.]126, hosted POWERTRASH malware

	connection to this domain.
zatravnik1[.]com	Resolves to 166.1.160[.]205, NetSupport RAT C2
01cp.txt	Filename for Active Directory information export
01ema.txt	Filename for Active Directory information export
01usr.txt	Filename for Active Directory information export
C:\ProgramData\Crosstec\client32.exe	Path on disk for NetSupport RAT
001c68b2f71d1fcb9cea1bc42ed0b4c2b6d9fce4b4754d05d6a5a1f28573373a	Malicious MSIX
1aec04bbf32d06b9cc032755c70103673f1137371a9d4f4608b4a309467943ed	Malicious PowerShell Script
1b63f83f06dbd9125a6983a36e0dbd64026bb4f535e97c5df67c1563d91eff89	NetSupport RAT
21903b51f23f7af681a9f69aa066753b202af6c537b97a247d98cfbdec150d63	NetSupport RAT
6ca002e77ed2c70dd265bea42b89d969	Malicious MSIX file
e14c3224215ea91587e96b995861e8966166dfc08ab4d409bd729770815b3b81	NetSupport RAT

	NetSupport RAT C2
193.233.22[.]126	Hosted malicious storageplace[.]pro domain, hosted POWERTRASH malware
94.131.107[.]181	Hosts typosquatted Grammarly domains

CLUSTER 2 INDICATORS OF COMPROMISE

IOC	CONTEXT
1204knos[.]ru	Python reached out to this domain
1204networks[.]ru	Python reached out to this domain
48aa2393ef590bab4ff2fd1e7d95af36e5b6911348d7674347626c9aaafa255e	Install.exe

CLUSTER 3 INDICATORS OF COMPROMISE

4sync[.]com	Malicious PowerShell reac out to this doma
623start[.]site	Malicious PowerShell reac out to this doma Resolves to 195.161.114[.]3
756-ads-info[.]xyz	Malicious PowerShell reac out to this doma
cdn-dwnld[.]ru	Resolves to 195.161.114[.]3, which is a ArechClient2 C2
clk-info[.]ru	Malicious PowerShell reac out to this doma Resolves to 81.177.140[.]69
eventbox[.]com	Resolves to 31.172.76[.]107, which is a ArechClient2 C2
fullpower682[.]store	Resolves to 81.177.140[.]69, h hosted ArechClient2 in past
next-traf623[.]site	Malicious Powershell reac out to this doma
notio-apps[.]cloud	Malicious

shaadidates[.]com	Malicious PowerShell reac out to this doma
tatmacerasi[.]com	Malicious domai associated with ArechClient2 an Redline
tombeaux-saadiens[.]com	PowerShell mad network connection to th domain
09b7d9976824237fc2c5bd461eab7a22	Malicious MSIX
1f64f01063b26bf05d4b076d54816e54dacd08b7fd6e5bc9cc5d11a548ff2215	This hash was se with two differen names: AcroBroker.exe and VBoxSVC.e Both binaries we signed by Adobe PDF Broker Proc for Internet Expl .
4f5e36e74b318c2aab027bc01e093f210a20e911dc5c15f7c6462d8243f09246	Malicious RAR downloaded fro fullpower682[.]s
5cf033157f63781a190b43d5dde427ccbe16ecda7cab4ccee617bd2d24e6a081	Malicious PowerShell scrip
7bef661ffc9788b5c54e0f98728f34155d7a713f2bfffeb0ef5dc7e33d52aca1	Redline Stealer
a58ebff4519a8af8ec4111e232be13b12bb41bf5f9a8bf9436ba6c5afe292f8f	Hash for a file named sqlite.dll was used in sear order hijacking

f5244c0d5c537efb24c9103e866eea26	Malicious MSIX
f57a22a7b0b28d0636cf0a9f79754778ea8660946db8236fcdab335d0335aec4	Malicious PowerShell scrip
185.197.75[.]191	ArechClient2 C
194.26.135[.]119	Malicious PowerShell reac out to this IP
195.161.114[.]3	ArechClient2 C
31.172.76[.]107	ArechClient2 C
77.246.101[.]46	Redline C2
81.177.140[.]69	This IP has hoste numerous malic domains, includi clk-info[.]ru and fullpower682[.]s
81.177.140[.]194	Hosts numerous malicious domai including next-traf623[.]site

CLUSTER 1 MITRE MAPPING

MITRE SUBTECHNIQUE	CATEGORY	EXAMPLE
T1204.002 User	Execution	Usage of malicious MSIX files

T1036.005 - Masquerading: Match Legitimate Name or Location	Defense Evasion	Malicious MSIX masquerade as legitimate Zoom, Microsoft Tean
T1570 - Lateral Tool Transfer	Lateral Movement	`"xcopy.exe" "C:\Users\\AppData\Roaming" "C:\Users\\AppData\Local\Packages\manager_c4g82jgbfsn1c /c /h /q /i /k`
T1059.001 - Command and Scripting Interpreter: PowerShell	Execution	`Powershell.exe -ExecutionPolicy RemoteSigned -file '.\k`
T1105 - Ingress Tool Transfer	Command and Control	Adversaries use PowerShell to load POWERTRASH and Carbanc
T1219 - Remote Access Software	Command and Control	Usage of NetSupport RAT
T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Persistence	Modifying AutoRun key at \registry\user\\software\microsoft\windows\currentversion\run\
T1069.002 Permission Groups Discovery: Domain Groups	Discovery	`net group "Domain Admins" /domain`
T1482 - Domain Trust Discovery	Discovery	`nltest /domain_trusts /all_trusts`

Domain Account		`samAccountName,description,info,mail,middleName,display`
		`-f 01usr.txt`

CLUSTER 2 MITRE MAPPING

MITRE SUBTECHNIQUE	CATEGORY	EXAMPLE
T1204.002 User Execution: Malicious File	Execution	Usage of malicious MSIX files
T1036.005 - Masquerading: Match Legitimate Name or Location	Defense Evasion	Malicious MSIX masquerade as legitimate Zoom, Microsoft Grammarly installers
T1059 - Command and Scripting Interpreter	Execution	Execution of malicious BAT, Python, and EXE files
T1047 - Windows Management Instrumentation T1046 Network Service Discovery	Execution Discovery	`wmic computersystem get domain`
T1033 - System Owner/User Discovery	Discovery	`whoami /groups`
T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Persistence	Modifying AutoRun key at \registry\user\\software\microsoft\windows\currentversio

T1140 Deobfuscate/Decode Files or Information	Defense Evasion	`openssl enc -aes-256-cbc -d -in code9.exe.enc -out pbkdf2 -pass pass:[redacted]`
T1562.001 - Impair Defenses: Disable or Modify Tools	Defense Evasion	Adversaries executed PowerShell commands to exclude W Defender from scanning the contents of various locations such as %TEMP%, %UserProfile%*, .bat and .ps1.

CLUSTER 3 MITRE MAPPING

MITRE SUBTECHNIQUE	CATEGORY	EXAMPLE
T1204.002 User Execution: Malicious File	Execution	Usage of malicious MSIX files
T1036.005 - Masquerading: Match Legitimate Name or Location	Defense Evasion	Malicious MSIX masquerade as legitimate Zoom, Microsoft Tea
T1570 - Lateral Tool Transfer	Lateral Movement	`"xcopy.exe" "C:\Program Files\WindowsApps\GoogleLLC.Chrome_115.0.5790.173_x64__ "C:\Users\\AppData\Local\Packages\GoogleLLC.Chrome_cvpb /e /s /y /c /h /q /i /k`
T1027.010 - Obfuscated Files or Information: Command Obfuscation	Defense Evasion	Adversaries used encoded PowerShell write malicious data to a

T1059.001 - Command and Scripting Interpreter: PowerShell	Execution	`Powershell.exe -ExecutionPolicy RemoteSigned -file 'C:\`
		`Files\WindowsApps\GoogleLLC.Chrome_115.0.5790.173_x64__`
		`_new_21.08.ps1`

T1574.002 - Hijack Execution Flow: DLL Side-Loading	Persistence, Privilege Escalation, Defense Evasion	Malicious vboxsvc.exe binary loaded a DLL named sqlite.dll.
T1518.001 - Software Discovery: Security Software Discovery	Discovery	Red Canary observed a malicious PowerShell script use WMI to endpoint.
T1555.003 - Credentials from Password Stores: Credentials from Web Browsers	Credential Access	Redline stealer and other infostealers steal credentials from wel
T1105 - Ingress Tool Transfer	Command and Control	Adversaries use PowerShell to download ArechClient2 or Redlin

RELATED ARTICLES

THREAT INTELLIGENCE

Intelligence Insights: October 2024

Intelligence Insights: September 2024

THREAT INTELLIGENCE

Recent dllFake activity shares code with SecondEye

THREAT INTELLIGENCE

Intelligence Insights: August 2024

Search

PRODUCTS

Managed Detection and Response (MDR)

Readiness Exercises

Linux EDR

Atomic Red Team™

Mac Monitor

What's New?

Plans

SOLUTIONS

Deliver Enterprise Security Across Your IT Environment

Get a 24×7 SOC Instantly

Protect Your Corporate Endpoints and Network

Protect Your Users' Email, Identities, and SaaS Apps

Protect Your Cloud

Protect Critical Production Linux and Kubernetes

Stop Business Email Compromise

Replace Your MSSP or MDR

Run More Effective Tabletops

Train Continuously for Real-World Scenarios

Operationalize Your Microsoft Security Stack

Minimize Downtime with After-Hours Support

RESOURCES

View all Resources

Blog

Integrations

Guides & Overviews

Cybersecurity 101

Case Studies

Videos

Webinars

Events

Customer Help Center

Newsletter

PARTNERS

Overview

Incident Response

Insurance & Risk

Managed Service Providers

Solution Providers

Technology Partners

Apply to Become a Partner

COMPANY

About Us

The Red Canary Difference

News & Press

Careers – We're Hiring!

Contact Us

Trust Center and Security