GALLIUM: Targeting global telecom

microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/

December 12, 2019

Microsoft Threat Intelligence Center (MSTIC) is raising awareness of the ongoing activity by a group we call GALLIUM, targeting telecommunication providers. When Microsoft customers have been targeted by this activity, we notified them directly with the relevant information they need to protect themselves. By sharing the detailed methodology and indicators related to GALLIUM activity, we're encouraging the security community to implement active defenses to secure the broader ecosystem from these attacks.

To compromise targeted networks, GALLIUM target unpatched internet-facing services using publicly available exploits and have been known to target vulnerabilities in WildFly/JBoss. Once persistence is established in a network, GALLIUM uses common techniques and tools like Mimikatz to obtain credentials that allows for lateral movement across the target network. Within compromised networks, GALLIUM makes no attempt to obfuscate their intent and are known to use common versions of malware and publicly available toolkits with small modifications. The operators rely on low cost and easy to replace infrastructure that consists of dynamic-DNS domains and regularly reused hop points.

This activity from GALLIUM has been identified predominantly through 2018 to mid-2019. GALLIUM is still active; however, activity levels have dropped when compared to what was previously observed.

Following Microsoft's internal practices of assigning chemical elements to activity groups, GALLIUM is the code name for this activity group.

GALLIUM's profile

Reconnaissance methods

As is often the case with the reconnaissance methods, it's difficult to be definitive about those employed by GALLIUM. This is due to the passive nature of reconnaissance activities by the actor including the use of freely available data from open sources, such as public websites and social media outlets. However, based on MSTIC analyst assessments, GALLIUM's exploitation of internet-facing services indicates it's likely they use open source research and network scanning tools to identify likely targets.

Delivery and exploitation

To gain initial access a target network, GALLIUM locates and exploits internet-facing services such as web servers. GALLIUM has been observed exploiting unpatched web services, such as WildFly/JBoss, for which exploits are widely available. Compromising a

web server gives GALLIUM a foothold in the victim network that doesn't require user interaction, such as traditional delivery methods like phishing.

Following exploitation of the web servers, GALLIUM actors typically install web shells, and then install additional tooling to allow them to explore the target network.

Lateral movement

GALLIUM uses a variety of tools to perform reconnaissance and move laterally within a target network. The majority of these are off-the-shelf tools or modified versions of known security tools. MSTIC investigations indicate that GALLIUM modifies its tooling to the extent it evades antimalware detections rather than develop custom functionality. This behavior has been observed with GALLIUM actors across several operational areas.

GALLIUM has been observed using several tools. Samples of the most prevalent are noted in Table 1.

Tool	Purpose
HTRAN	Connection bouncer to proxy connections.
Mimikatz	Credential dumper.
NBTScan	Scanner for open NETBIOS nameservers on a local or remote TCP/IP network.
Netcat	Reads from and writes to network connections using TCP or UDP protocols.
PsExec	Executes a command line process on a remote machine.
Windows Credential Editor (WCE)	Credential dumper.
WinRAR	Archiving utility.

Table 1: GALLIUM tooling.

GALLIUM has signed several tools using stolen code signing certificates. For example, they've used a credential dumping tool signed using a stolen certificate from *Whizzimo, LLC*, as shown in Figure 1. The code signing certificate shown in Figure 1 was no longer valid at the time of writing; however, it shows GALLIUM had access to such certificates.

Figure 1. Credential dumping tool signed using a stolen Whizzimo, LLC certificate.

GALLIUM primarily relies on compromised domain credentials to move through the target network, and as outlined above, uses several credential harvesting tools. Once they have acquired credentials, the activity group uses PsExec extensively to move laterally between hosts in the target network.

Installation

GALLIUM predominantly uses widely available tools. In certain instances, GALLIUM has modified these tools to add additional functionality. However, it's likely these modifications have been made to subvert antimalware solutions since much of the malware and tooling employed by GALLIUM is historic and is widely detected by security products. For example, QuarkBandit is a modified version of the widely used Gh0st RAT, an openly available remote access tool (RAT). Similarly, GALLIUM has made use of a modified version of the widely available Poison Ivy RAT. These RATs and the China Chopper web shell form the basis of GALLIUM's toolkit for maintaining access to a victim network.

Infrastructure

GALLIUM predominantly uses dynamic DNS subdomains to provide command and control (C2) infrastructure for their malware. Typically, the group uses the ddns.net and myftp.biz domains provided by noip.com. MSTIC analysis indicates the use of dynamic DNS providers as opposed to registered domains is in line with GALLIUM's trend towards low cost and low effort operations.

GALLIUM domains have been observed hosted on infrastructure in mainland China, Hong Kong SAR, and Taiwan.

When connecting to web shells on a target network GALLIUM has been observed employing Taiwan-based servers. Observed IP addresses appear to be exclusive to GALLIUM, have little to no legitimate activity, and are reused in multiple operations. These servers provide

high fidelity pivot points during an investigation.

A package of GALLIUM indicators containing GALLIUM command and control domains used during this operation have been prepared for Azure Sentinel and is available on the Microsoft GitHub.

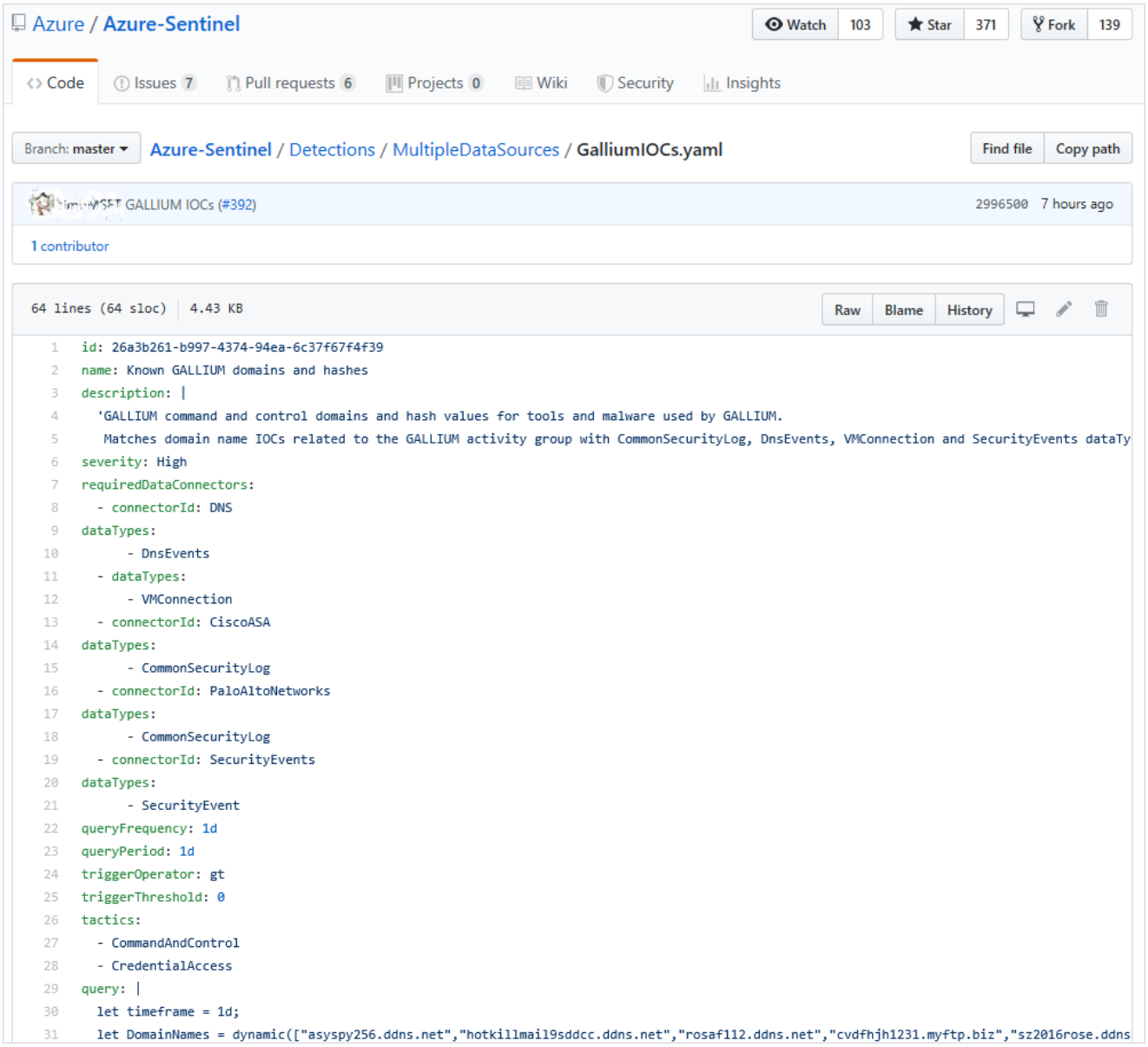

Figure 2. Azure Sentinel query of GALLIUM indicators.

GALLIUM use of malware

First stage

GALLIUM does not typically use a traditional first stage installer for their malware. Instead, the group relies heavily on web shells as a first method of persistence in a victim network following successful exploitation. Subsequent malware is then delivered through existing web shell access.

Microsoft Defender Advanced Threat Protection (ATP) exposes anomalous behavior that indicate web shell installation and post compromise activity by analysing script file writes and process executions. Microsoft Defender ATP offers a number of detections for web shell activity protecting customers not just from GALLIUM activity but broader web shell activity too. Read the full report in your Microsoft Defender ATP portal.

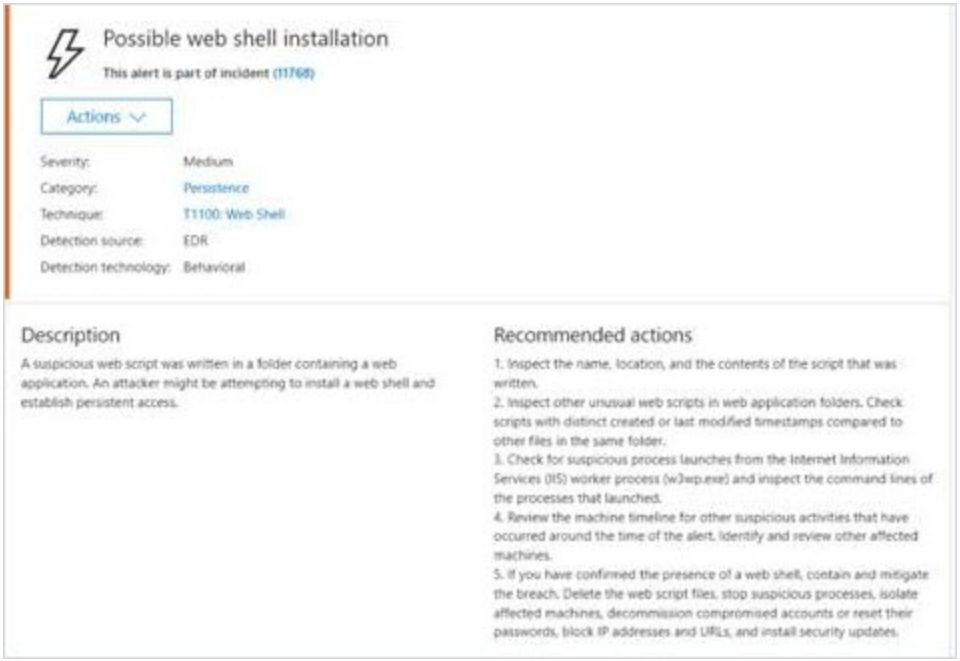

Figure 3. Microsoft Defender ATP web shell detection.

When alerted of these activities, the security operations team can then use the rich capabilities in Microsoft Defender ATP to investigate web shell activity and subsequent reconnaissance and enumeration activity to resolve web shell attacks.

Figure 4. Microsoft Defender ATP web shell process tree.

In addition to standard China Chopper, GALLIUM has been observed using a native web shell for servers running Microsoft IIS that is based on the China Chopper web shell; Microsoft has called this "BlackMould."

BlackMould contains functionality to perform the following tasks on a victim host:

- Enumerate local drives.
- Employ basic file operations like find, read, write, delete, and copy.
- Set file attributes.
- Exfiltrate and infiltrate files.
- Run cmd.exe with parameters.

Commands are sent in the body of HTTP POST requests.

Second stage

In cases where GALLIUM has deployed additional malware on a victim network, they've used versions of the Gh0st RAT (modified Ghost RAT detected as QuarkBandit) and Poison Ivy malware. In both cases, GALLIUM has modified the communication method used by the malware, likely to prevent detection through existing antimalware signatures since both malware families have several detections based on their original communication methods. Malware families are noted in Table 2.

Malware family	Description and primary usage
BlackMould	Native IIS web shell based on the China Chopper web shell.
China Chopper	Commonly used and widely shared web shell used by several threat actors. Not unique to GALLIUM.
Poison Ivy (modified)	Poison Ivy is a widely shared remote access tool (RAT) first identified in 2005. While Poison Ivy is widely used, the variant GALLIUM has been observed using is a modified version that appears to be unique to GALLIUM.
QuarkBandit	Gh0st RAT variant with modified configuration options and encryption.

Table 2. GALLIUM malware families.

GALLIUM's malware and tools appear to be highly disposable and low cost. In cases where GALLIUM has invested in modifications to their toolset, they appear to focus on evading antimalware detection, likely to make the malware and tooling more effective.

The MSTIC team works closely with Microsoft security products to implement detections and protections for GALLIUM malware and tooling in a number of Microsoft products. Figure 4 shows one such detection for a GALLIUM PoisonIvy loader in Microsoft Defender ATP.

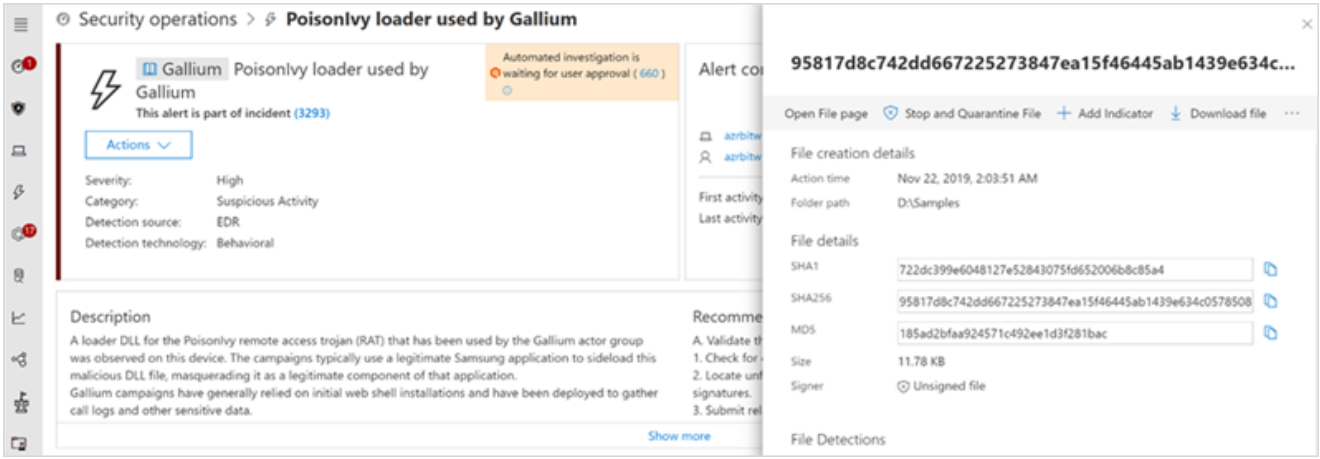

Figure 5. GALLIUM PoisonIvy loader in Microsoft Defender ATP.

Additionally, MSTIC has authored a number of antimalware signatures for Windows Defender Antivirus covering the aforementioned malware families, a list of GALLIUM exclusive signature can be found in the Related indicators" section.

In addition to these malware families, GALLIUM has been observed employing SoftEther VPN software to facilitate access and maintain persistence to a target network. By installing SoftEther on internal systems, GALLIUM is able to connect through that system as though they are on the internal network of the target. SoftEther provides GALLIUM with another means of persistence and flexibility with the added benefit that its traffic may appear to be benign on the target network.

Recommended defenses

The following are recommended defenses security operations teams can take to mitigate the impact of threats like GALLIUM in your corporate environment:

- Maintain web server patching and log audits, run web services with minimum required operating system permissions
- Install security updates on all applications and operating systems promptly. Check the Security Update Guide for detailed information about available Microsoft security updates.
- For efficient incident response, maintain a forensics-ready network with centralized event logging, file detonation services, and up-to-date asset inventories.
- Enable cloud-delivered protection and maintain updated antivirus.
- Turn on cloud-delivered protection and automatic sample submission on Windows Defender Antivirus. These capabilities use artificial intelligence (AI) and machine learning to quickly identify and stop new and unknown threats.
- Use behavior detection solutions to catch credential dumping or other activity that may indicate a breach.

- Adopt Azure ATP—a cloud-based security solution that leverages your on-premises Active Directory signals—to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
- Use Microsoft Defender ATP to help enterprise networks prevent, detect, investigate, and respond to advanced threats. Educate users about protecting personal and business information in social media, filtering unsolicited communication, identifying lures in spear-phishing email and watering holes, and reporting of reconnaissance attempts and other suspicious activity.
- Encourage users to use Microsoft Edge and other web browsers that support SmartScreen, which identifies and blocks malicious websites, including phishing sites, scam sites, and sites that contain exploits and host malware.
- Institute Multi-Factor Authentication (MFA) to mitigate against compromised accounts.
    - **Note**: Microsoft strongly encourages all customers download and use passwordless solutions like the Microsoft Authenticator app or Windows Hello to secure your accounts.
    - For Office 365 users, see MFA support.
    - For consumer and personal email accounts, see how to use two-step verification.

Related indicators

The list below provides known GALLIUM tooling and Indicators of Compromise (IOCs) observed during this activity. Microsoft encourages customers to implement detections and protections to identify possible prior campaigns or prevent future campaigns against their systems.

Tooling

Tool	Purpose
HTRAN	Connection bouncer to proxy connections.
Mimikatz	Credential dumper.
NBTScan	Scanner for open NETBIOS nameservers on a local or remote TCP/IP network.
Netcat	Reads from and writes to network connections using TCP or UDP protocols.
PsExec	Executes a command line process on a remote machine.
Windows Credential Editor (WCE)	Credential dumper.
WinRAR	Archiving utility.

Malware

Malware	Notes
BlackMould	Native IIS version of the China Chopper web shell.
China Chopper	Commonly used and widely shared web shell used by several threat actors. Not unique to GALLIUM.
Poison Ivy (modified)	Poison Ivy is a widely shared remote access tool (RAT) first identified in 2005. While Poison Ivy is widely used, the variant GALLIUM has been observed using is a modified version which appears to be unique to GALLIUM.
QuarkBandit	Gh0st RAT variant with modified configuration options and encryption.

Indicators

Indicator	Type
asyspy256[.]ddns[.]net	Domain
hotkillmail9sddcc[.]ddns[.]net	Domain
rosaf112[.]ddns[.]net	Domain
cvdfhjh1231[.]myftp[.]biz	Domain
sz2016rose[.]ddns[.]net	Domain
dffwescwer4325[.]myftp[.]biz	Domain
cvdfhjh1231[.]ddns[.]net	Domain
9ae7c4a4e1cfe9b505c3a47e66551eb1357affee65bfefb0109d02f4e97c06dd	Sha256
7772d624e1aed327abcd24ce2068063da0e31bb1d5d3bf2841fc977e198c6c5b	Sha256
657fc7e6447e0065d488a7db2caab13071e44741875044f9024ca843fe4e86b5	Sha256
2ef157a97e28574356e1d871abf75deca7d7a1ea662f38b577a06dd039dbae29	Sha256
52fd7b90d7144ac448af4008be639d4d45c252e51823f4311011af3207a5fc77	Sha256
a370e47cb97b35f1ae6590d14ada7561d22b4a73be0cb6df7e851d85054b1ac3	Sha256
5bf80b871278a29f356bd42af1e35428aead20cd90b0c7642247afcaaa95b022	Sha256
6f690ccfd54c2b02f0c3cb89c938162c10cbeee693286e809579c540b07ed883	Sha256
3c884f776fbd16597c072afd81029e8764dd57ee79d798829ca111f5e170bd8e	Sha256
1922a419f57afb351b58330ed456143cc8de8b3ebcbd236d26a219b03b3464d7	Sha256

fe0e4ef832b62d49b43433e10c47dc51072959af93963c790892efc20ec422f1	Sha256
7ce9e1c5562c8a5c93878629a47fe6071a35d604ed57a8f918f3eadf82c11a9c	Sha256
178d5ee8c04401d332af331087a80fb4e5e2937edfba7266f9be34a5029b6945	Sha256
51f70956fa8c487784fd21ab795f6ba2199b5c2d346acdeef1de0318a4c729d9	Sha256
889bca95f1a69e94aaade1e959ed0d3620531dc0fc563be9a8decf41899b4d79	Sha256
332ddaa00e2eb862742cb8d7e24ce52a5d38ffb22f6c8bd51162bd35e84d7ddf	Sha256
44bcf82fa536318622798504e8369e9dcdb32686b95fcb44579f0b4efa79df08	Sha256
63552772fdd8c947712a2cff00dfe25c7a34133716784b6d486227384f8cf3ef	Sha256
056744a3c371b5938d63c396fe094afce8fb153796a65afa5103e1bffd7ca070	Sha256
TrojanDropper:Win32/BlackMould.A!dha	Signature Name
Trojan:Win32/BlackMould.B!dha	Signature Name
Trojan:Win32/QuarkBandit.A!dha	Signature Name
Trojan:Win32/Sidelod.A!dha	Signature Name

Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us at @MSFTSecurity for the latest news and updates on cybersecurity.