Microsoft Security—detecting empires in the cloud

microsoft.com/en-us/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/

September 24, 2020

By Microsoft Threat Intelligence Center
Microsoft Threat Intelligence Center

Microsoft consistently tracks the most advanced threat actors and evolving attack techniques. We use these findings to harden our products and platform and share them with the security community to help defenders everywhere better protect the planet.

Recently, the Microsoft Threat Intelligence Center (MSTIC) observed the evolution of attacker techniques by an actor we call GADOLINIUM using cloud services and open source tools to enhance weaponization of their malware payload, attempt to gain command and control all the way to the server, and to obfuscate detection. These attacks were delivered via spear-phishing emails with malicious attachments and detected and blocked by Microsoft Defender, formerly Microsoft Threat Protection (MTP), and able to be detected using Azure Sentinel.

As these attacks were detected, Microsoft took proactive steps to prevent attackers from using our cloud infrastructure to execute their attacks and suspended 18 Azure Active Directory applications that we determined to be part of their malicious command & control infrastructure. This action helped transparently protect our customers without requiring additional work on their end.

GADOLINIUM is a nation-state activity group that has been compromising targets for nearly a decade with a worldwide focus on the maritime and health industries. As with most threat groups, GADOLINIUM tracks the tools and techniques of security practitioners looking for new techniques they can use or modify to create new exploit methods.

Recently, MSTIC has observed newly expanded targeting outside of those sectors to include the Asia Pacific region and other targets in higher education and regional government organizations. As GADOLINIUM has evolved, MSTIC has continued to monitor its activity and work alongside our product security teams to implement customer protections against these attacks.

Historically, GADOLINIUM used custom-crafted malware families that analysts can identify and defend against. In response, over the last year GADOLINIUM has begun to modify portions of its toolchain to use open-source toolkits to obfuscate their activity and make it more difficult for analysts to track. Because cloud services frequently offer a free trial or one-time payment (PayGo) account offerings, malicious actors have found ways to take advantage of these legitimate business offerings. By establishing free or PayGo accounts, they can use cloud-based technology to create a malicious infrastructure that can be established quickly then taken down before detection or given up at little cost.

The following GADOLINIUM technique profile is designed to give security practitioners who may be targeted by this specific actor's activity insight and information that will help them better protect from these attacks.

2016: Experimenting in the cloud

GADOLINIUM has been experimenting with using cloud services to deliver their attacks to increase both operation speed and scale for years. The image in Figure 1 is from a GADOLINIUM controlled Microsoft TechNet profile established in 2016. This early use of a TechNet profiles' contact widget involved embedding a very small text link that contained an encoded command for malware to read.

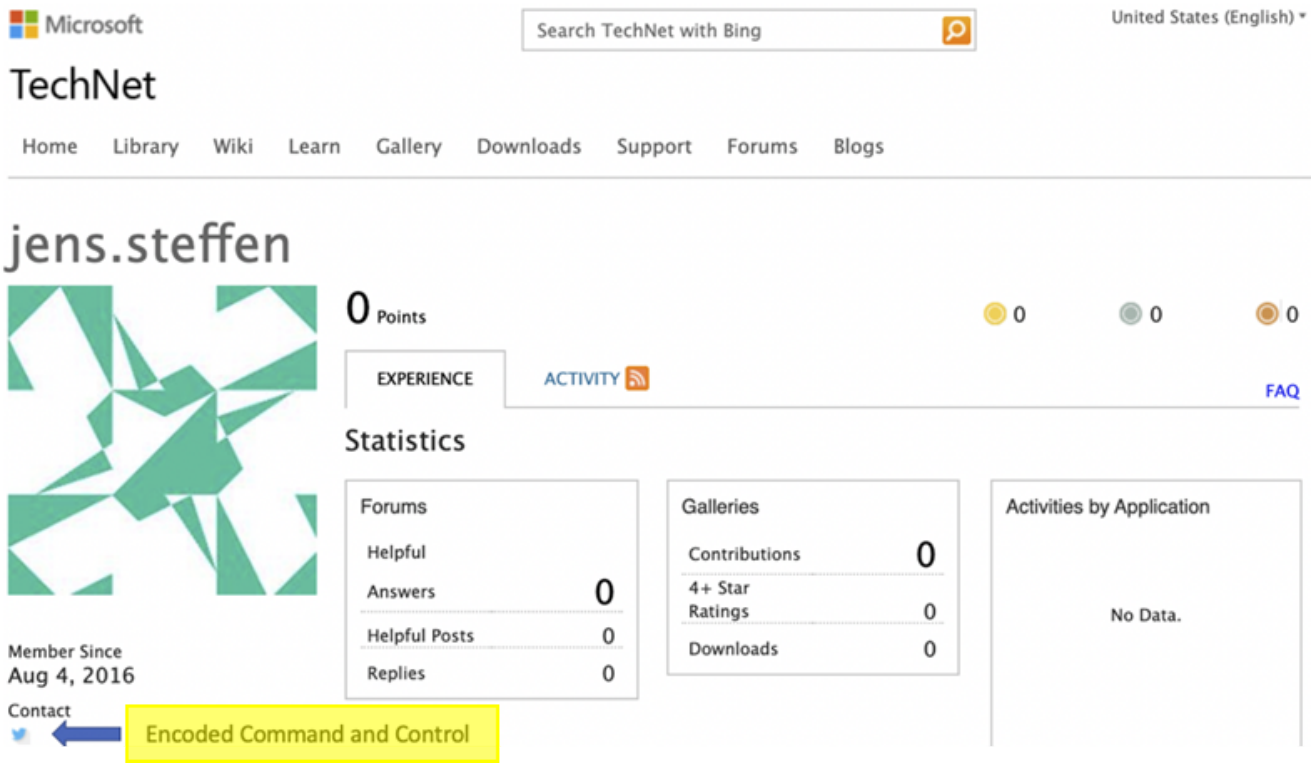


Figure 1: GADOLINIUM controlled TechNet profile with embedded malware link.

2018: Developing attacks in the cloud

In 2018 GADOLINIUM returned to using Cloud services, but this time it chose to use GitHub to host commands. The image in Figure 2 shows GitHub Commit history on a forked repository GADOLINIUM controlled. In this repository, the actors updated markdown text to issue new commands to victim computers. MSTIC has worked with our colleagues at GitHub to take down the actor accounts and disrupt GADOLINIUM operations on the GitHub platform.

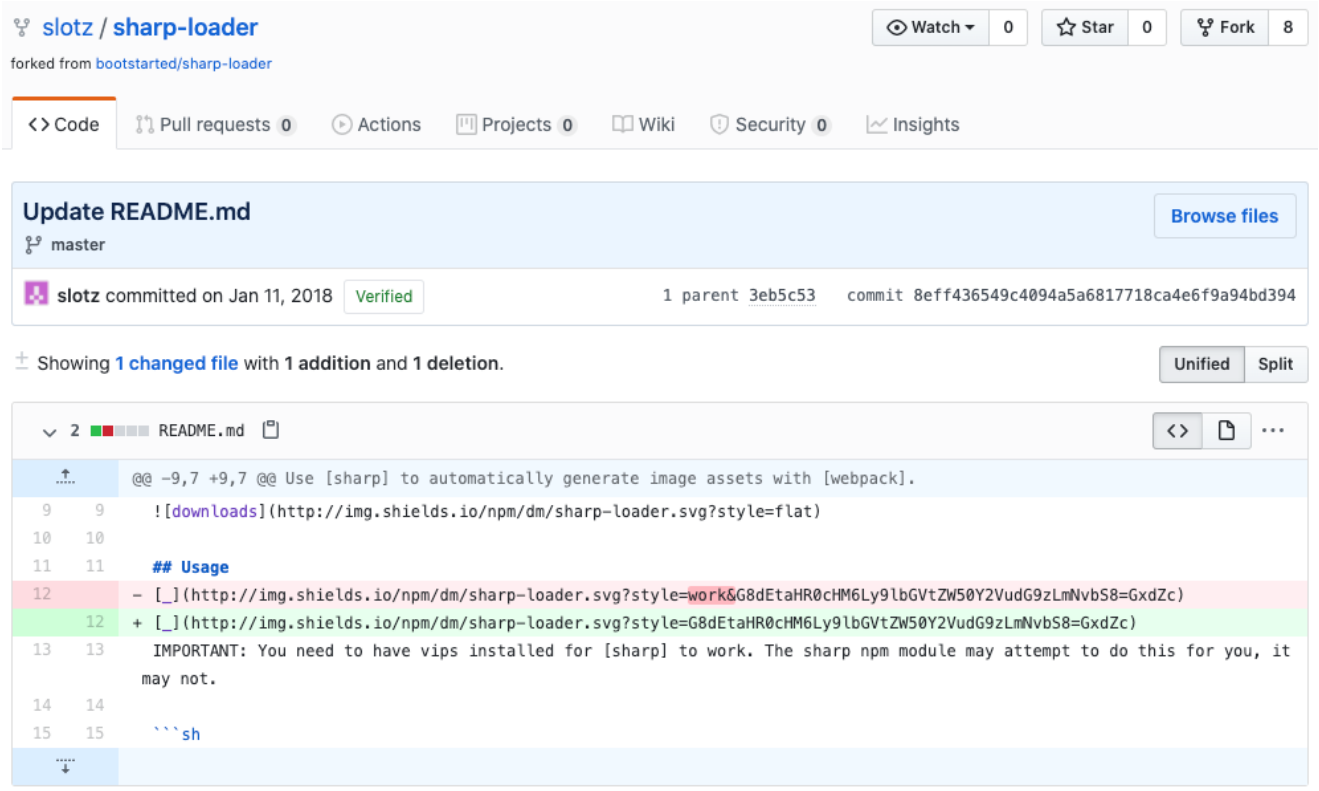
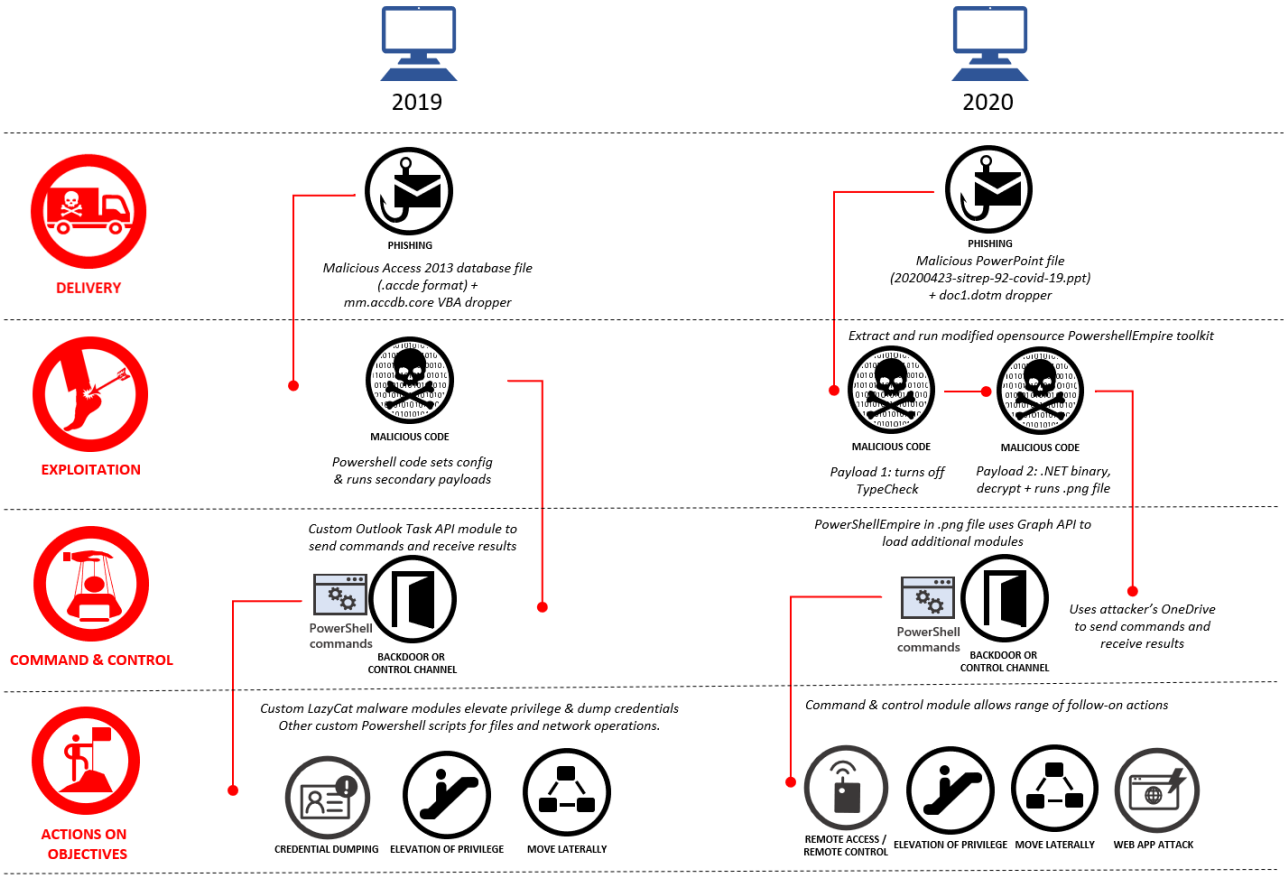


Figure 2: GitHub repository controlled by GADOLINIUM.

2019-2020: Hiding in plain sight using open source

GADOLINIUM's evolving techniques

Two of the most recent attack chains in 2019 and 2020 were delivered from GADOLINIUM using similar tactics and techniques. Below is a summary view of how these attacks techniques have evolved followed by a detailed analysis of each step that security practitioners can use to better understand the threat and what defenses to implement to counter the attacks.



Weaponization

In the last year, Microsoft has observed GADOLINIUM migrate portions of its toolchain techniques based on open source kits. GADOLINIUM is not alone in this move. MSTIC has noticed a slow trend of several nation-state activity groups migrating to open source tools in recent years. MSTIC assesses this move is an attempt to make discovery and attribution more difficult. The other added benefit to using open-source types of kits is that the development and new feature creation is done and created by someone else at no cost. However, using open source tools isn't always a silver bullet for obfuscation and blending into the noise.

Delivery & Exploitation (2019)

In 2019, we discovered GADOLINIUM delivering malicious Access database files to targets. The initial malicious file was an Access 2013 database (.accde format). This dropped a fake Word document that was opened along with an Excel spreadsheet and a file called *mm.accdb.core* which was subsequently executed. The file *mm.accdb.core* is a VBA dropper, based on the CactusTorch VBA module, which loads a .NET DLL payload, sets configuration information, and then runs the payload. Defender for Office 365 detects and blocks malicious Microsoft Access database attachments in email. A redacted example of the configuration is displayed below.

```
entry_class = "Class1"
Set o = d.DynamicInvoke(al.ToArray()).CreateInstance(entry_class)
o.ClientID = "8b48b31a-8cb4-48f2-9077-5a93e4f23442"
o.UserName = "Joe.Bloggs@outlook.com"
o.Password = "OnjaU907(jajb"
o.Secret = "iubnknbk55%20Alss;"
o.Run "VBA"
```

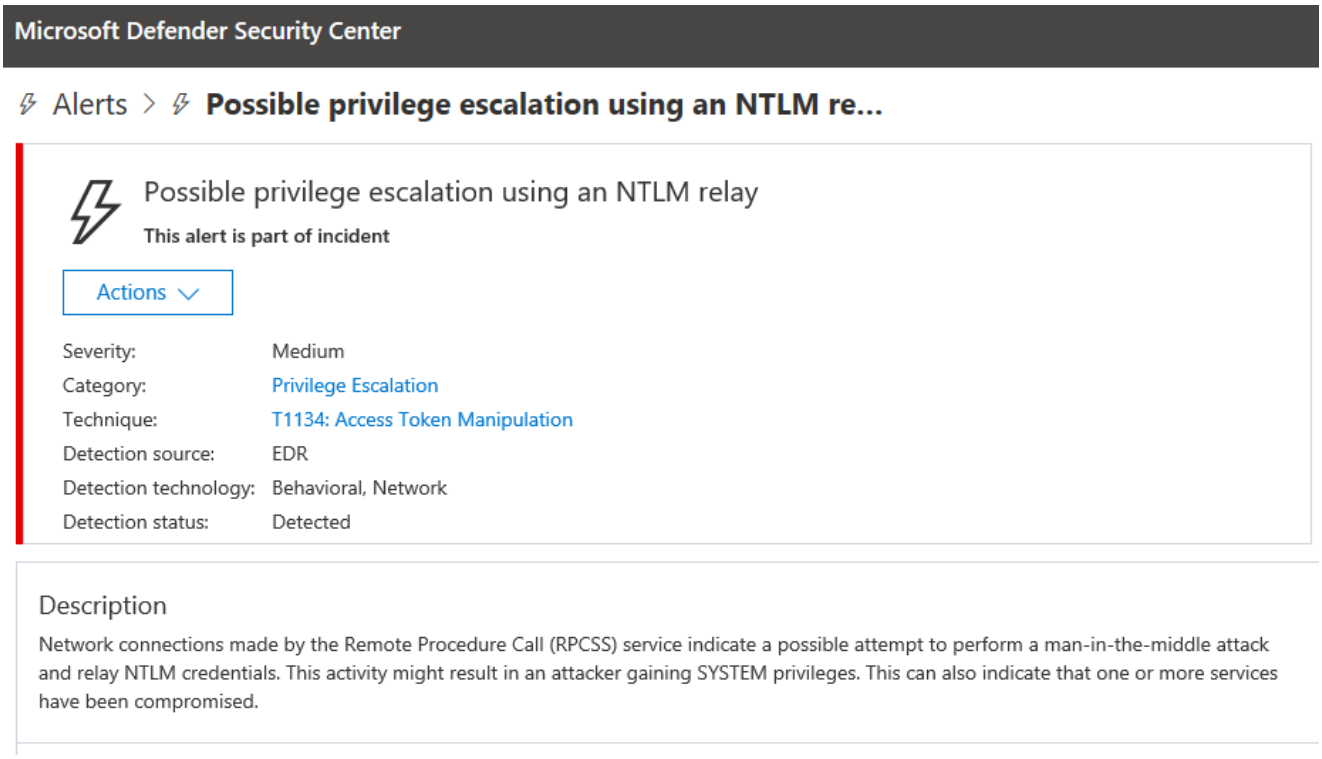
Figure 3: VBA setting config and calling the "Run" function of the payload

Command and Control (2019)
Having gained access to a victim machine the payload then uses attachments to Outlook Tasks as a mechanism for command and control (C2). It uses a GADOLINIUM-controlled OAuth access token with login.microsoftonline.com and uses it to call the Outlook Task API to check for tasks. The attacker uses attachments to Outlook tasks as a means of sending commands or .NET payloads to execute; at the victim end, the malware adds the output from executing these commands as a further attachment to the Outlook task.

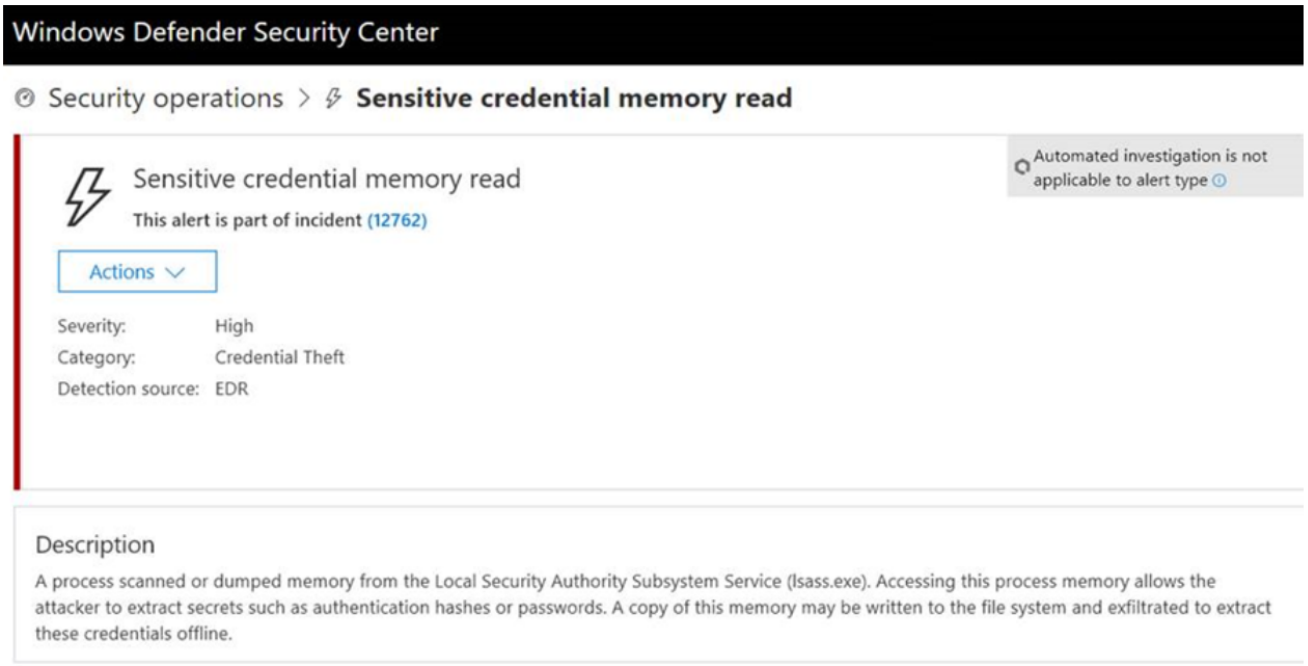
Interestingly, the malware had code compiled in a manner that doesn't seem to be used in the attacks we saw. In addition to the Outlook Tasks API method described above, the extra code contains two other ways of using Office365 as C2, via either the Outlook Contacts API (get and add contacts) or the OneDrive API (list directory, get and add a file).

Actions on Objective (2019)
GADOLINIUM used several different payloads to achieve its exploitation or intrusion objectives including a range of PowerShell scripts to execute file commands (read/write/list etc.) to enable C2 or perform SMB commands (upload/download/delete etc.) to potentially exfiltrate data.

LazyCat, one of the tools used by GADOLINIUM, includes privilege escalation and credential dumping capability to enable lateral movement across a victim network. Microsoft Defender for Endpoint detects the privilege escalation technique used:



LazyCat performs credential dumping through usage of the *MiniDumpWriteDump* Windows API call, also detected by Microsoft Defender for Endpoint:



Delivery (2020)

In mid-April 2020 GADOLINIUM actors were detected sending spear-phishing emails with malicious attachments. The filenames of these attachments were named to appeal to the target's interest in the COVID-19 pandemic. The PowerPoint file (*20200423-sitrep-92-covid-*

19.ppt), when run, would drop a file, *doc1.dotm*. Similarly, to the 2019 example, Microsoft Defender for Office detects and blocks emails with these malicious PowerPoint and Word attachments.

Command and Control (2020)
The malicious doc1.dotm had two payloads which run in succession.

- The first payload turns off a type check *DisableActivitySurrogateSelectorTypeCheck* which the second stage needs as discussed in this blog.
- The second payload loads an embedded .Net binary which downloads, decrypts + runs a .png file.

The .png is actually PowerShell which downloads and uploads fake png files using the Microsoft Graph API to *https://graph.microsoft.com/v1.0/drive/root:/onlinework/contact/$($ID)_1.png:/content* where $ID is the ID of the malware. The GADOLINIUM PowerShell is a modified version of the opensource PowershellEmpire toolkit.

Actions on Objectives (2020)
The GADOLINIUM PowerShell Empire toolkit allows the attacker to load additional modules to victim computers seamlessly via Microsoft Graph API calls. It provides a command and control module that uses the attacker's Microsoft OneDrive account to execute commands and retrieve results between attacker and victim systems. The use of this PowerShell Empire module is particularly challenging for traditional SOC monitoring to identify. The attacker uses an Azure Active Directory application to configure a victim endpoint with the permissions needed to exfiltrate data to the attacker's own Microsoft OneDrive storage. From an endpoint or network monitoring perspective the activity initially appears to be related to trusted applications using trusted cloud service APIs and, in this scenario,, no OAuth permissions consent prompts occur. Later in this blog post, we will provide additional information about how Microsoft proactively prevents attackers from using our cloud infrastructure in these ways.

Command and Control—Server compromise
GADOLINIUM campaigns often involve installing web shells on legitimate web sites for command and control or traffic redirection. Microsoft Defender for Endpoint detects web shells by analyzing web server telemetry such as process creation and file modifications. Microsoft blogged earlier in the year on the use of web shells by multiple groups and how we detect such activities.

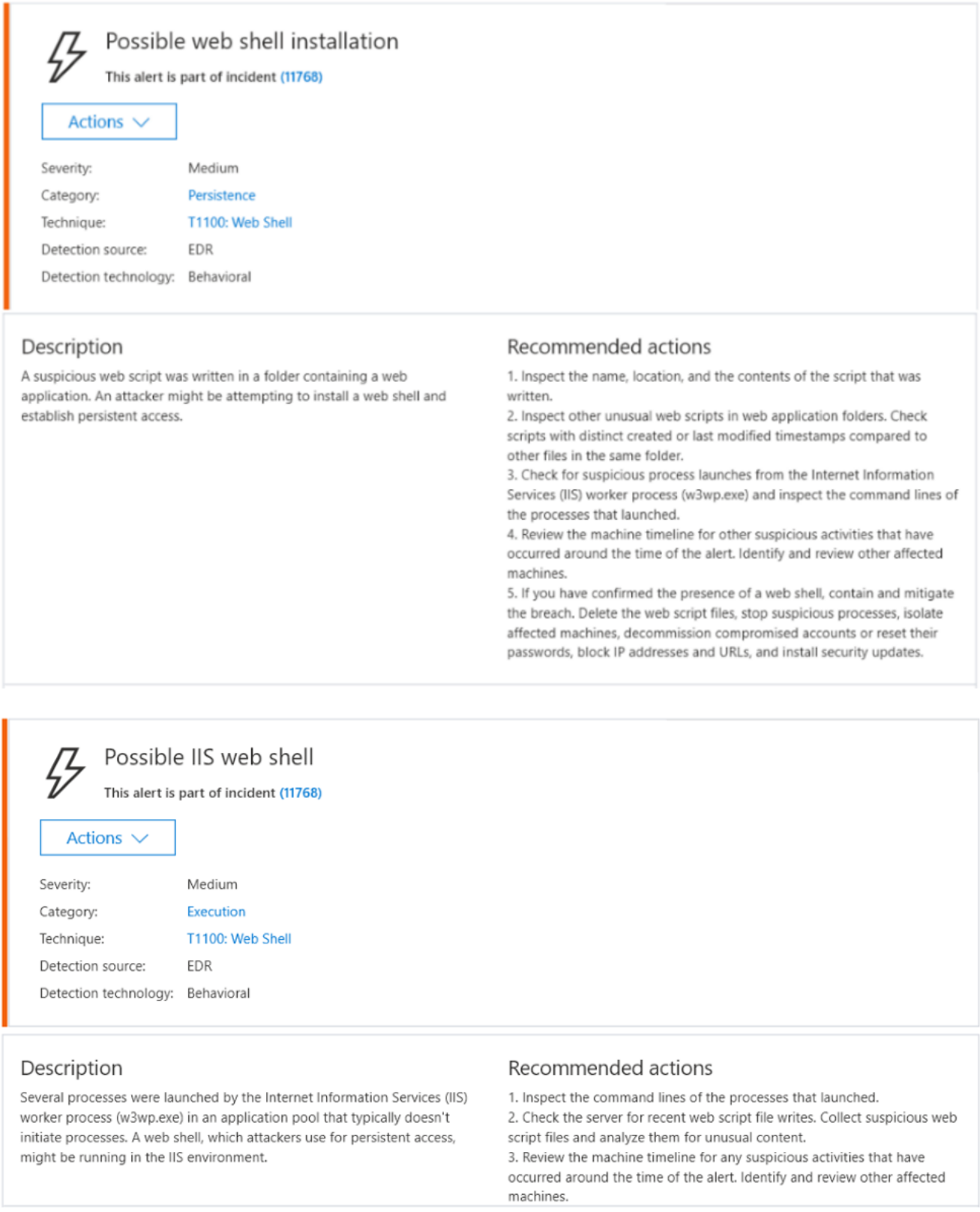


Figure 6: Microsoft Defender for Endpoint alerts of suspicious web shell attacks.

Web shell alerts from Microsoft Defender for Endpoint can be explored in Azure Sentinel and enriched with additional information that can give key insights into the attack. MSTIC's Azure Sentinel team recently published a blog outlining how such insights can be derived by

analyzing events from the W3CIISLog.

Microsoft's proactive steps to defend customers
In addition to detecting many of the individual components of the attacks through Microsoft's security products and services such as Microsoft Defender for Endpoint and for Microsoft Defender for Office as described above, we also take proactive steps to prevent attackers from using our cloud infrastructure to perpetrate attacks. As a cloud provider, Microsoft is uniquely positioned to disrupt this attacker technique. The PowerShell Empire scenario is a good example of this. During April 2020, the Microsoft Identity Security team suspended 18 Azure Active Directory applications that we determined to be part of GADOLINIUM's PowerShell Empire infrastructure (Application IDs listed in IOC section below). Such action is particularly beneficial to customers as suspending these applications protects all customers transparently without any action being required at their end.)

As part of Microsoft's broader work to foster a secure and trustworthy app ecosystem, we research and develop detection techniques for both known and novel malicious applications. Applications exhibiting malicious behavior are quickly suspended to ensure our customers are protected.

GADOLINIUM will no doubt evolve their tactics in pursuit of its objectives. As those threats target Microsoft customers, we will continue to build detections and implement protections to defend against them. For security practitioners looking to expand your own hunting on GADOLINIUM, we are sharing the below indicators of compromise (IOCs) associated with their activity.

List of related GADOLINIUM indicators

Hashes from malicious document attachments

faebff04d7ca9cca92975e06c4a0e9ce1455860147d8432ff9fc24622b7cf675
f61212ab1362dffd3fa6258116973fb924068217317d2bc562481b037c806a0a

Actor-owned email addresses

Chris.sukkar@hotmail.com
PhillipAdamsthird@hotmail.com
sdfwfde234sdws@outlook.com
jenny1235667@outlook.com
fghfert32423dsa@outlook.com
sroggeveen@outlook.com
RobertFetter.fdmed@hotmail.com
Heather.mayx@outlook.com

Azure Active Directory App IDs associated with malicious apps

ae213805-a6a2-476c-9c82-c37dfc0b6a6c
afd7a273-982b-4873-984a-063d0d3ca23d
58e2e113-b4c9-4f1a-927a-ae29e2e1cdeb
8ba5106c-692d-4a86-ad3f-fc76f01b890d
be561020-ba37-47b2-99ab-29dd1a4312c4
574b7f3b-36da-41ee-86b9-c076f999b1de
941ec5a5-d5bf-419e-aa93-c5afd0b01eff
d9404c7d-796d-4500-877e-d1b49f02c9df
67e2bb25-1f61-47b6-9ae3-c6104e587882
9085bb9e-9b56-4b84-b21e-bd5d5c7b0de0
289d71ad-54ee-44a4-8d9a-9294f19b0069
a5ea2576-4191-4e9a-bfed-760fff616fbf
802172dc-8014-42a9-b765-133c07039f9f
fb33785b-f3f7-4b2b-b5c1-f688d3de1bde
c196c17d-1e3c-4049-a989-c62f7afaf7f3
79128217-d61e-41f9-a165-e06e1d672069
f4a41d96-2045-4d75-a0ec-9970b0150b52
88d43534-4128-4969-b5c4-ceefd9b31d02

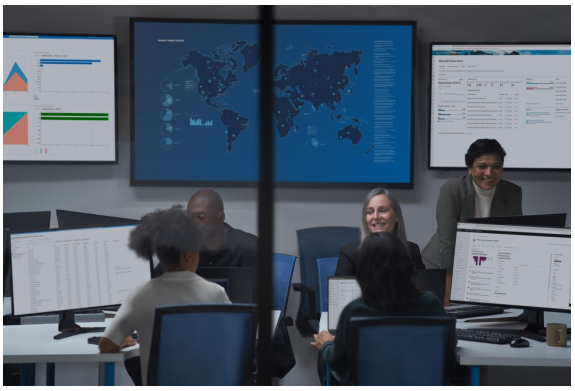
To learn more about Microsoft Security solutions visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us at @MSFTSecurity for the latest news and updates on cybersecurity.

Related Posts

Research
Threat intelligence
Threat actors
Feb 216 min read

2022 in review: DDoS attack trends and insights

With DDoS attacks becoming more frequent, sophisticated, and inexpensive to launch, it's important for organizations of all sizes to be proactive and stay protected. In this blog, we detail trends and insights into DDoS attacks we observed and mitigated throughout 2022.



Detecting malicious key extractions by compromised identities for Azure Cosmos DB

Azure Cosmos DB is a fully managed NoSQL cloud database service for modern app development. It offers a variety of advanced built-in features, such as automatic worldwide data replication, lightning-fast response types, and a variety of APIs. In this blog post, we describe security practices for securing access to Azure Cosmos DB and show how monitoring relevant control plane operations can help in the detection of potentially compromised authorization.

Securing your IoT with Edge Secured-core devices

To simplify your IoT security journey, today, we're announcing the availability of Windows IoT Edge Secured-core devices available in the Azure Certified Device catalog from Lenovo, ASUS and AAEON, additionally we're also announcing the availability of devices that meet the Microsoft sponsored Edge Compute Node protection profile which is governed with industry oversight, from Scalys and Eurotech. And learn more on Microsoft's investments in MCU security.

Anatomy of a DDoS amplification attack

Amplification attacks are one of the most common distributed denial of service (DDoS) attack vectors. These attacks are typically categorized as flooding or volumetric attacks, where the attacker succeeds in generating more traffic than the target can process, resulting in exhausting its resources due to the amount of traffic it receives.