Critical Attack Discovery and Intelligence Team
Symantec

POSTED: 10 OCT, 2018 | 6 MIN READ | THREAT INTELLIGENCE

Gallmaker: New Attack Group Eschews Malware to Live off the Land

A new attack group is targeting government, military, and defense sectors in what appears to be a classic espionage campaign.

UPDATE October 11, 2018

This blog has been updated with a revised list of IoCs. An earlier list of IOCs attached to this blog was generated through an automated system and, due to the dual-use nature of the tools used by the group, erroneously included some low fidelity IoCs.

Symantec researchers have uncovered a previously unknown attack group that is targeting government and military targets, including several overseas embassies of an Eastern European country, and military and defense targets in the Middle East. This group eschews custom malware and uses living off the land (LotL) tactics and publicly available hack tools to carry out activities that bear all the hallmarks of a cyber espionage campaign.

The group, which we have given the name Gallmaker, has been operating since at least December 2017, with its most recent activity observed in June 2018.

Tactics and tools

The most interesting aspect of Gallmaker's approach is that the group doesn't use malware in its operations. Rather, the attack activity we observed is carried out exclusively using LotL tactics and publicly available hack tools. The group takes a number of steps to gain access to a victim's device and then deploys several different attack tools, as follows:

1. The group delivers a malicious Office lure document to victims, most likely via a spear-phishing email.
2. These lure documents use titles with government, military, and diplomatic themes, and the file names are written in English or Cyrillic languages. These documents are not very sophisticated, but evidence of infections shows that they're effective. The attackers use filenames that would be of interest to a variety of targets in Eastern Europe, including:

- *bg embassy list.docx*
- *Navy.ro members list.docx*

3. These lure documents attempt to exploit the Microsoft Office Dynamic Data Exchange (DDE) protocol in order to gain access to victim machines. When the victim opens the lure document, a warning appears asking victims to "enable content" *(See Figure 1)*. Should a user enable this content, the attackers are then able to use the DDE protocol to remotely execute commands in memory on the victim's system. By running solely in memory, the attackers avoid leaving artifacts on disk, which makes their activities difficult to detect.
4. Once the Gallmaker attackers gain access to a device, they execute various tools, including:

- WindowsRoamingToolsTask: Used to schedule PowerShell scripts and tasks.
- A "reverse_tcp" payload from Metasploit: The attackers use obfuscated shellcode that is executed via PowerShell to download this reverse shell.
- A legitimate version of the WinZip console: This creates a task to execute commands and communicate with the command-and-control (C&C) server. It's likely this WinZip console is used to archive data, probably for exfiltration.
- The Rex PowerShell library, which is publicly available on GitHub, is also seen on victim machines. This library helps create and manipulate PowerShell scripts for use with Metasploit exploits.

Gallmaker is using three primary IP addresses for its C&C infrastructure to communicate with infected devices. There is also evidence that it is deleting some of its tools from victim machines once it is finished, to hide traces of its activity.

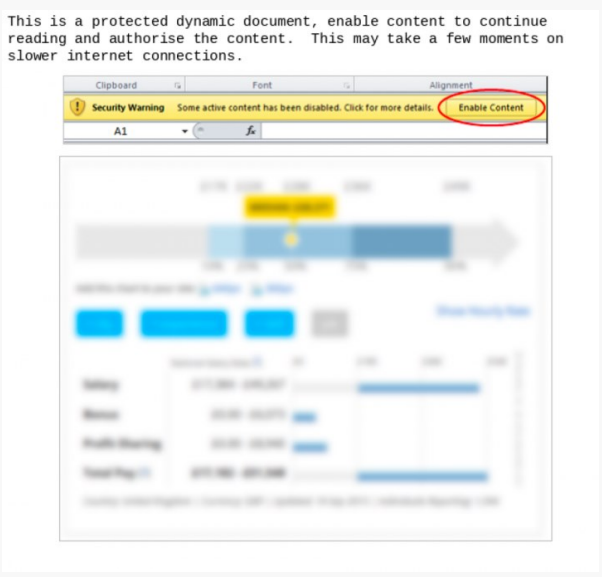

Figure 1. An example of the type of warning displayed by the lure document

The DDE protocol can be used for legitimate purposes to send messages between Microsoft applications that share data through shared memory, e.g. to share data between Excel and Word.

However, the DDE protocol was flagged as unsecure last year, when researchers discovered it could be exploited to execute code on victim machines via Excel and Word, without macros being enabled in those applications. Microsoft said at the time that this capability was a feature and the company did not consider it a vulnerability because Office always warned users before enabling DDE in documents, as seen in Figure 1. However, after the DDE protocol was subsequently exploited in a number of malware campaigns, Microsoft issued an update to Office in December 2017 that disabled DDE by default in Word and Excel. DDE can be enabled manually after this update is applied but only if the registry is altered by an admin account.

The Gallmaker victims we have seen did not have this patch installed and therefore were still vulnerable to exploit via the DDE protocol.

Targets and timeline

Gallmaker's activity appears to be highly targeted, with its victims all related to government, military, or defense sectors. Several targets are embassies of an Eastern European country. The targeted embassies are located in a number of different regions globally, but all have the same home country.

The other targets we have seen are a Middle Eastern defense contractor and a military organization. There are no obvious links between the Eastern European and Middle Eastern targets, but it is clear that Gallmaker is specifically targeting the defense, military, and government sectors: its targets appear unlikely to be random or accidental.

Gallmaker's activity has been quite consistent since we started tracking it. The group has carried out attacks most months since December 2017. Its activity subsequently increased in the second quarter of 2018, with a particular spike in April 2018.

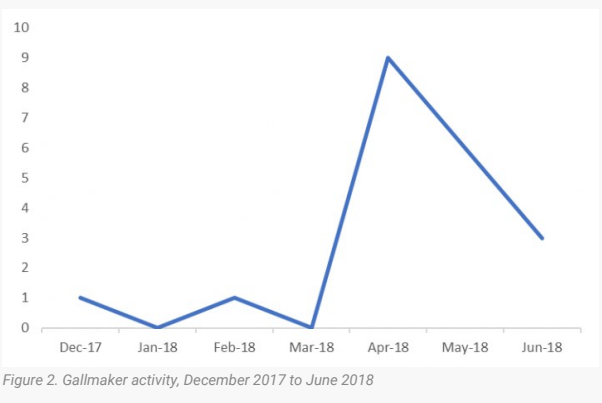

Figure 2. Gallmaker activity, December 2017 to June 2018

Gallmaker's activity points strongly to it being a cyber espionage campaign, likely carried out by a state-sponsored group.

> Gallmaker may well have continued to avoid detection were it not for Symantec's Targeted Attack Analytics (TAA) technology.

How did we discover Gallmaker?

The fact that Gallmaker appears to rely exclusively on LotL tactics and publicly available hack tools makes its activities extremely hard to detect. We have written extensively about the increasing use of LotL tools and publicly available hack tools by cyber criminals. One of the primary reasons for the increased popularity of these kinds of tools is to avoid detection; attackers are hoping to "hide in plain sight", with their malicious activity hidden in a sea of legitimate processes.

Gallmaker may well have continued to avoid detection were it not for Symantec's Targeted Attack Analytics (TAA) technology. TAA combines the capabilities of Symantec's world-leading security experts with advanced artificial intelligence and machine learning to provide organizations with their own "virtual analysts", via our Advanced Threat Protection (ATP) product. Since its inception, TAA has detected security incidents at thousands of organizations, automating what would have taken many hours of analyst time. In this instance, TAA identified the specific PowerShell commands used by Gallmaker as being suspicious, leading to the discovery of this new campaign. Without TAA's advanced AI-based capabilities, Gallmaker's activities may well have remained undetected.

Protection

The following protections are in place to protect customers against Gallmaker attacks:

- System Infected: Meterpreter Reverse TCP
- W97M.Downloader

Network protection products also detect activity associated with Gallmaker.

Indicators of Compromise

The following indicators are specific to Gallmaker:

Network

- 111[.]90.149.99/o2
- 94[.]140.116.124/o2
- 94[.]140.116.231/o2

Filenames

- bg embassy list.docx
- Navy.ro members list.docx
- БГ в чуждите медии 23.03.2018-1.docx
- [REDACTED] and cae join forces to develop integrated live virtual constructive training solutions.docx
- A-9237-18-brasil.docx

Gallmaker also used tools that were available in open source projects. Yara rule and methods shared below were used by Gallmaker but aren't exclusive to the group's activity. Detection of these in one's environment is only indicative of possible unauthorized activity. Each occurrence of triggers must be examined to determine intent.

rule Suspicious_docx
{
meta:
copyright = "Symantec"
family = "Suspicious DOCX"
group = "Gallmaker"
description = "Suspicious file that might be Gallmaker"

strings:
$quote = /<w:fldSimple w:instr=" QUOTE (([^"]+)* [0-9]

{2,3}

)

{4}

/
$text = "select \"Update field\" and click \"OK\""

condition:
any of them
}

Use of Rex Powershell - https://github.com/rapid7/rex-powershell

Use of obfuscated shellcode executed via PowerShell to download a "reverse_tcp" payload from Metasploit onto victim systems. For example, msfvenom -p windows/meterpreter/reverse_tcp -o payload.bin

Further reading

To find out more about TAA, read our whitepaper: Targeted Attack Analytics: Using Cloud-based Artificial Intelligence for Enterprise-Focused Advanced Threat Protection.