THREAT ALERT: Emotet Targeting Japanese Organizations

By Cybereason Global SOC Team

Archived: 2026-04-05 14:01:57 UTC

The Cybereason Global Security Operations Center (SOC) issues Cybereason Threat Alerts to inform customers of emerging impacting threats. The Alerts summarize these threats and provide practical recommendations for protecting against them.

What's Happening?

The Cybereason GSOC is investigating a significant surge of infections with the Emotet malware in Japan. In the last quarter of 2021, for the first time since early 2021, when authorities disrupted the infrastructure of Emotet operators, the Cybereason GSOC observed global attack campaigns that involved a then-new variant of Emotet.

The surge of Emotet targeting Japanese organizations in the first quarter of 2022 is a continuation of the earlier Emotet activity, with some changes in the malware deployment process.

Key Observations

- The Emotet malware poses a significant threat to users' privacy and security. There is a significantly high rate of infections with the Emotet malware in Japan in the first quarter of 2022.
- In contrast to the Emotet attack scenarios that the Cybereason GSOC observed in the last quarter of 2021, the scenarios that the Cybereason GSOC is observing at the time of writing this article do not involve PowerShell for deploying Emotet on systems.
- The Cybereason XDR Platform detects and prevents the Emotet malware.

Analysis

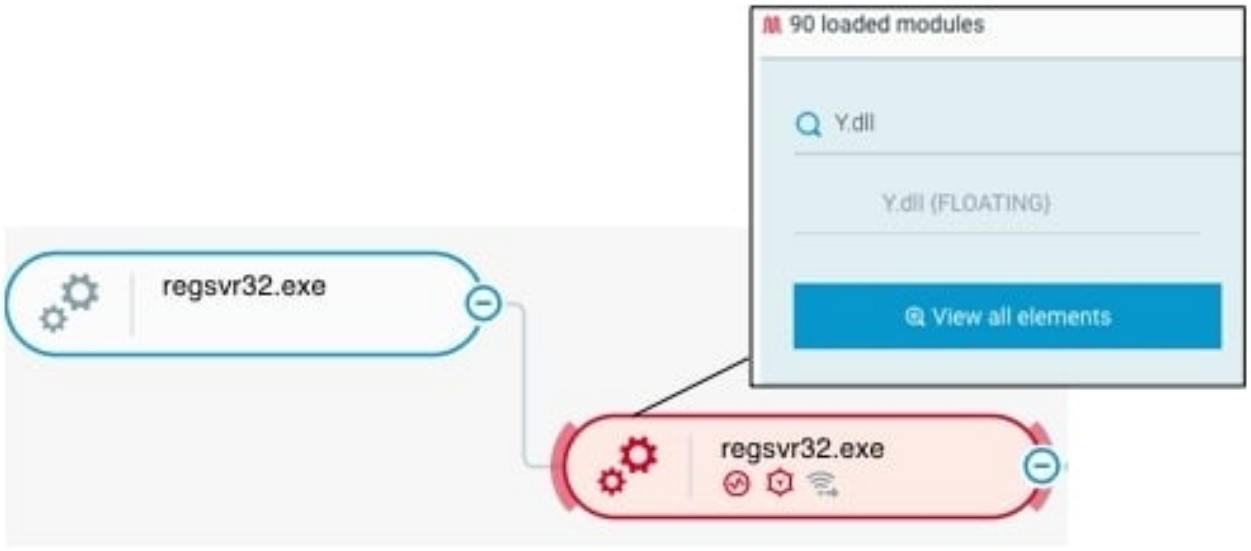
Malicious actors distribute Emotet as attachments (Microsoft Excel documents) to phishing emails. The Excel documents store malicious Office macros that distribute Emotet. When the Office macros execute, the macros establish a connection to an attacker-controlled endpoint to download the Emotet malware.

Emotet typically arrives from the attacker-controlled endpoint in the form of a dynamic-link library (DLL) file that the macros store as a file with the filename extension **.ocx**, such as **xxw1.ocx** or **enu.ocx**. The Office macros use the **regsvr32** Windows utility to execute Emotet (the DLL file with the extension **.ocx)** through the **DllRegisterServer** DLL entry point. Emotet then copies the Emotet DLL file to a file with a random filename that is stored:

- In the user's **%AppData%** folder, if Emotet executes with normal user privileges, such as **C:\Users\user\AppData\Local\Jcvshzvga\xfofujkytigar.pum**.

- In the **%SystemRoot%\SYSWOW64** folder, if Emotet executes with administrative privileges, such as **C:\Windows\SysWOW64\Fkyrhqgbvmjinn\nugiehweexgz.liz**.

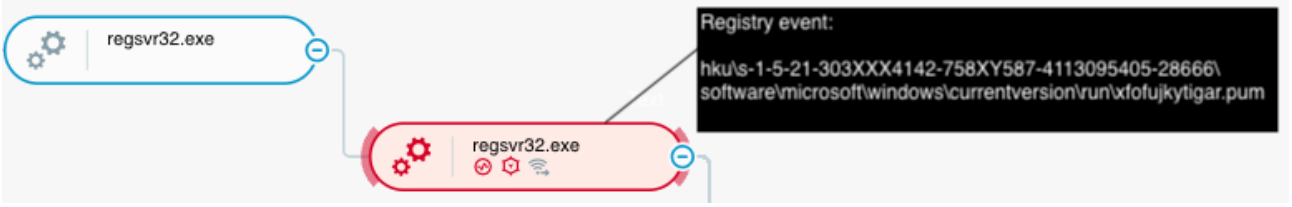
Emotet then executes the copied Emotet DLL file with the **regsvr32** Windows utility. We observed that **regsvr32** maps the Emotet DLL under the internal name of **Y.dll**. Users of the Cybereason XDR Platform can view this name as the name of a module that executes in the context of **regsvr32**:



rundll32 maps an Emotet DLL file under the internal name of Y.dll as seen in the Cybereason XDR Platform

We emphasize that in contrast to the Emotet attack scenarios that the Cybereason GSOC observed in the last quarter of 2021, the scenarios that the Cybereason GSOC is observing at the time of writing this article (the first quarter of 2022) do not involve PowerShell for deploying Emotet on systems.

When Emotet executes on a compromised system, the malware first establishes persistence by creating system services that start at system startup or creating registry values at the **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run** registry key:



Emotet (DLL file: xfofujkytigar.pum) establishes persistence on a compromised system as seen in the Cybereason XDR Platform

Emotet then executes processes that conduct malicious activities, such as reconnaissance (for example, **ipconfig.exe** or **systeminfo.exe**) or stealing web and email credentials from client credential databases.

For example, as we discussed in a previous research, Emotet uses the keyword **scomma** in the command line to execute **WebBrowserPassView,** a tool that steals web credentials from browser credential databases.

Most of the processes that Emotet executes have random names and are children processes of the **regsvr32** process that executes Emotet:

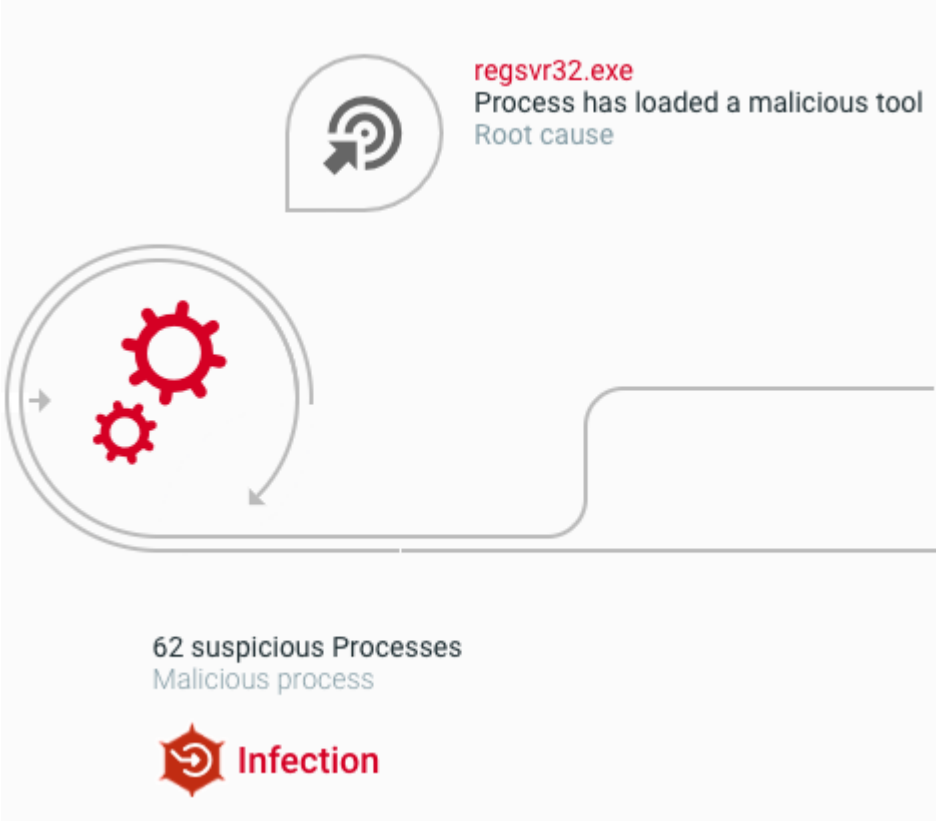
Emotet executes processes that conduct malicious activities (Emotet executes the WebBrowserPassView tool) as seen in the Cybereason XDR Platform

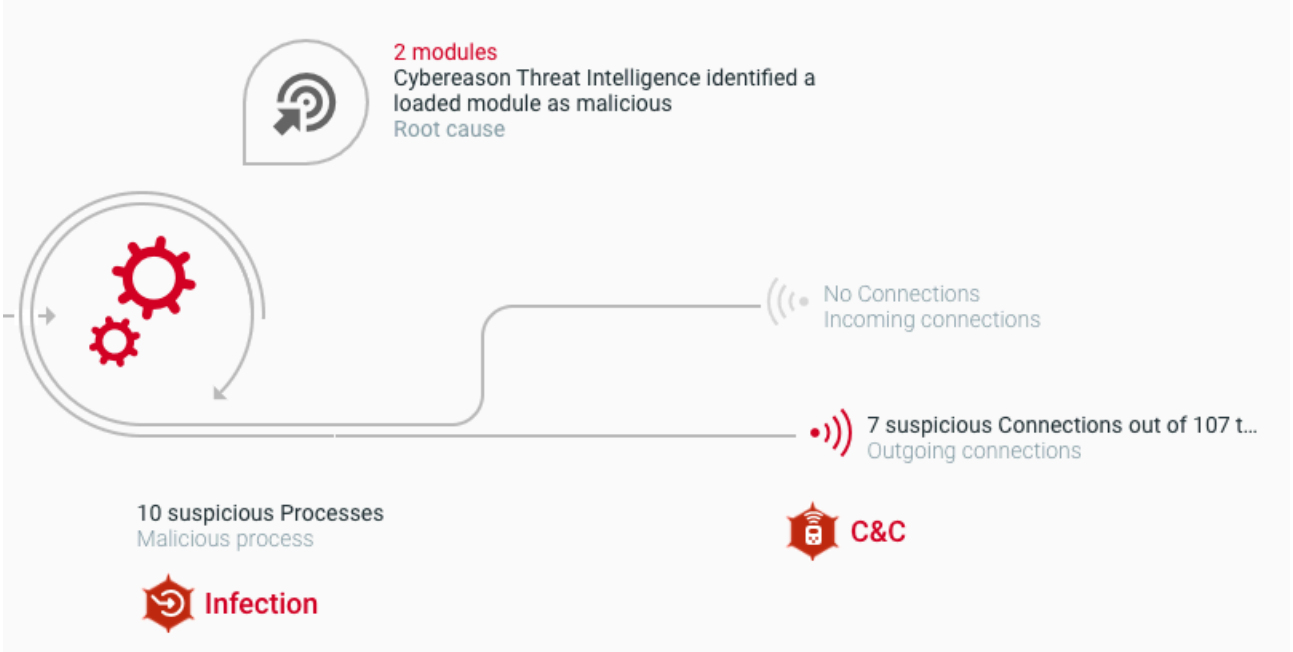
Cybereason Recommendations

The Cybereason XDR Platform detects and prevents the Emotet malware. Cybereason recommends the following:

- Securely handle email messages and attachments that originate from external sources. This includes investigating email message content to identify phishing attempts.

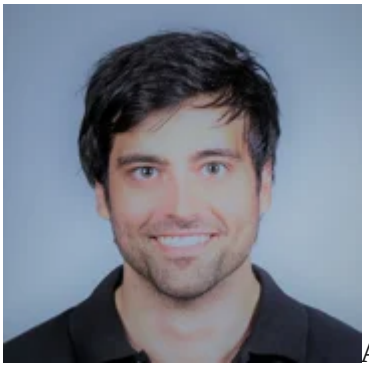
- Use secure passwords, regularly rotate passwords, and use multi-factor authentication where possible.
- In the Cybereason XDR Platform, enable **Application Control** to block the execution of malicious files.
- Threat Hunting with Cybereason: The Cybereason MDR team provides its customers with custom hunting queries for detecting specific threats - to find out more about threat hunting and [Managed Detection and Response] with the Cybereason Defense Platform, [contact a Cybereason Defender here].
    - For Cybereason customers: More details [available on the NEST] including custom threat hunting queries for detecting this threat:





The Cybereason XDR Platform detects the Emotet malware

About the Researcher:



Aleksandar Milenkoski, Senior Malware and Threat Analyst, Cybereason Global SOC

Aleksandar Milenkoski is a Senior Malware and Threat Analyst with the Cybereason Global SOC team. He is involved primarily in reverse engineering and threat research activities. Aleksandar has a PhD in system security. For his research activities, he has been awarded by SPEC (Standard Performance Evaluation Corporation), the Bavarian Foundation for Science, and the University of Würzburg, Germany. Prior to Cybereason, his work focused on research in intrusion detection and reverse engineering security mechanisms of the Windows operating system.

About the Author

Cybereason Global SOC Team

The Cybereason Global SOC Team delivers 24/7 Managed Detection and Response services to customers on every continent. Led by cybersecurity experts with experience working for government, the military and multiple industry verticals, the Cybereason Global SOC Team continuously hunts for the most sophisticated and pervasive threats to support our mission to end cyberattacks on the endpoint, across the enterprise, and everywhere the battle moves.

All Posts by Cybereason Global SOC Team
