SORINTSEC

THREAT HUNTING

LAB

WEEK 15/12/2025 - 19/12/2025

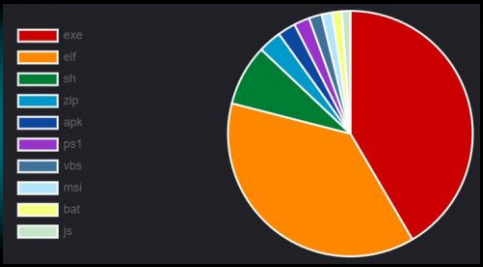
PUBLIC

Index

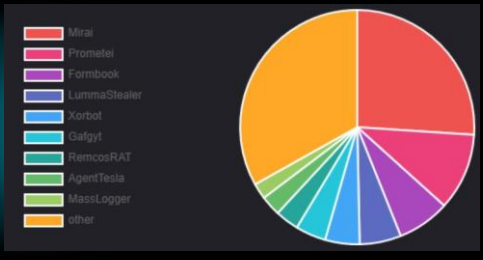
Global Weekly Threat Overview

Multiple threat actors are compromising Microsoft 365 accounts in phishing attacks that leverage the OAuth device code authorization mechanism. Attackers trick victims into entering a device code on Microsoft's legitimate device login page, unknowingly authorizing an attacker-controlled application and granting them access to the target account without stealing credentials or bypassing multi-factor authentication (MFA). Although the method isn't new, email security firm Proofpoint says that these attacks have increased significantly in volume since September, and involve both financially motivated cybercriminals like TA2723 and state-aligned threat actors.

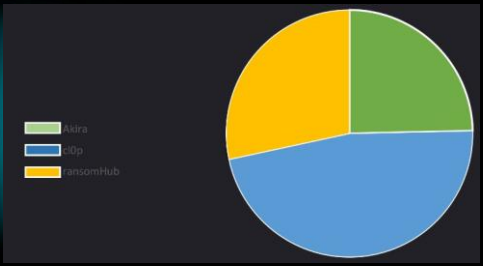
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



A malicious package in the Node Package Manager (NPM) registry poses as a legitimate WhatsApp Web API library to steal WhatsApp messages, collect contacts, and gain access to the account. A fork of the popular WhiskeySockets Baileys project, the malicious package provides the legitimate functionality. It has been available on npm published under the name lotusbail for at least six months and has accumulated more than 56,000 downloads. Researchers at supply-chain security company Koi Security discovered the malicious package and found that it could steal WhatsApp authentication tokens and session keys, intercept and record all messages - both sent and received, and exfiltrate contact lists, media files, and documents.

Global Weekly Notable One

Modify Registry: Persistence

Fancy Bear, also known as APT28 or Sofacy, is a Russian state-sponsored cyber-espionage group linked to Russia's military intelligence service, the GRU's Unit 26165, active since the mid-2000s.

It targets NATO governments, military entities, critical infrastructure, and political organizations through spear-phishing, zero-days, and custom malware for persistent access and data theft. Notable operations include the 2016 DNC hack, Bundestag breaches, and WADA attacks to influence elections and expose secrets. The group adapts quickly with rotating C2, proxies, and anti-forensic tactics, prioritizing espionage and information warfare against Western interests.

Global Weekly Notable One

The NotDoor campaign, also known as GONEPOSTAL, is a sophisticated espionage operation attributed to the Russian-linked threat group Fancy Bear (APT28). Primarily targeting organizations in NATO member countries, the campaign utilizes a novel Outlook backdoor based on malicious VBA macros, based on Cordyceps backdoor plugin system developed in 2017 by researcher Greg Linares (AKA Laughing Mantis). Attackers initiate the infection by leveraging a legitimate Microsoft OneDrive.exe binary to facilitate DLL side-loading of a tampered SSPICLI.dll.

This loader establishes persistence by modifying Windows registry keys to force macro execution on boot and suppress security warnings. Once active, the malware monitors incoming emails for trigger words such as "Daily Report". Using email as a covert command-and-control channel, it can execute shell commands, upload files, and exfiltrate data. Finally, the malware leverages Outlook's event-driven architecture and custom string encoding to mask its operations and execute code stealthily.

Threat Hunting Activity

SORINTSEC

TACTIC

Persistence

TECHNIQUES

T1112 – Modify Registry

The adversary is trying to maintain their foothold. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as interact with the Windows Registry.

Threat Hunting Activity

The NotDoor campaign leverages the legitimate Microsoft OneDrive.exe binary to facilitate DLL side-loading. Attackers place a malicious, unsigned SSPICLI.dll in the same directory, which the signed binary loads to initiate the infection chain.

Modules:

Module	Address	Size	Path	Company
OneDrive.exe	0x7ff619750000	0x4cc000	C:\Users\5hid\Desktop\New folder\OneDrive.exe	Microsoft Corpor...
wininet.dll	0x7ffe4f8f0000	0x4dd000	C:\Windows\System32\wininet.dll	Microsoft Corpor...
secur32.dll	0x7ffe50ee0000	0xc000	C:\Windows\System32\secur32.dll	Microsoft Corpor...
version.dll	0x7ffe548b0000	0xa000	C:\Windows\System32\version.dll	Microsoft Corpor...
SSPICLI.dll	0x7ffe582a0000	0xc000	C:\Users\5hid\Desktop\New folder\SSPICLI.dll	

Malicious SSPICLI.dll side-load lab test

This rogue DLL maintains stealth by forwarding legitimate library functions to a renamed version of the original file. Once active, the DLL's code modifies registry keys such as LoadMacroProviderOnBoot to force automatic macro execution and bypass security warnings.

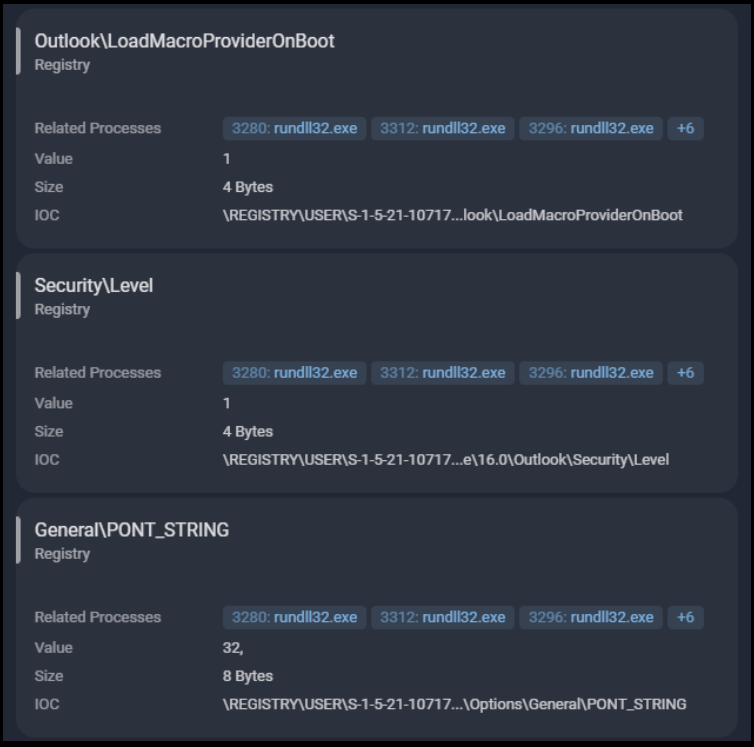
RegSetKeyValueW API call is the primary mechanism used by the malicious SSPICLI.dll to programmatically manipulate the Windows registry. This function is executed within the DLLMain execution path, specifically during the second half of the loader's routine, to dismantle security barriers and ensure the malicious VBA macros run without interruption.

```
int64_t* var_58;
sub_180001d60(&var_58, u"LoadMacroProviderOnBoot");
sub_180001d60(&var_78, u"Software\Microsoft\Office\16.0\Outlook");
int32_t data = 1;
int64_t* lpValueName = &var_58;
int64_t var_40;

if (var_40 > 7)
    lpValueName = var_58;

PWSTR lpSubKey = &var_78;

if (var_60_3 > 7)
    lpSubKey = (uint64_t)var_78;

RegSetKeyValueW(-0xffffffff80000001, lpSubKey, lpValueName, 4, &data, 4);
```

RegSetKeyValue(W) API call

Threat Hunting Activity

RegSetKeyValueW function sets the data for a specified value in a registry key and subkey. If the specified subkey does not exist, the API is designed to create it automatically. In this campaign, the attackers provide the following parameters to the API: hKey, the malware specifically targets the HKEY_CURRENT_USER hive; lpSubKey directed toward paths associated with Microsoft Outlook 16.0, such as Software\Microsoft\Office\16.0\Outlook and its security and general options subkeys; lpValueName and lpData to set three critical values that facilitate the backdoor: "LoadMacroProviderOnBoot" set to 1 to force Outlook to load the macro provider every time the application starts; "Level" set to 1 to lower the macro security level to "enable all macros" bypassing the standard "disable all macros with notification" setting and "PONT_STRING" set to "32" to suppress dialogue boxes that would normally warn a user when content is being downloaded from internet.



Registry keys modified during execution

By utilizing this function, the malware avoids manual user interaction and ensures that its persistence mechanism is active before the user even opens an email. This programmatic approach allows the loader to maintain a low profile, as these modifications are performed silently in the background using the Advapi32.dll library.

Threat Hunting Activity

Detection can be made monitoring modification in these specific registry keys path.

regkey_written	Outlook\LoadMacroProviderOnBoot
regkey_written	Security\Level
regkey_written	General\PONT_STRING

regkey_write events

Correlating events, by detecting this behavior, we are able to intercept activities potentially attributable to the observed campaign, as well as proceed with reactive hunting and identify potential infrastructures compromised by the campaign.

PUBLIC