THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

Cyber Threat Advisory

DragonOK

Threat Actor Malware

CATEGORY

Malware

SEVERITY

High

Platforms

Windows

IMPACT

- Modify Registry
- Process Injection
- Data Staged
- Command and Scripting Interpreter
- Hijack Execution Flow
- Modify Registry

Description

DragonOK

This campaign consisted of five distinct phishing attacks, each distributing a different variant of Sysget malware, also known as HelloBridge. The malware was attached to emails with the intent of deceiving recipients into opening it. This deception involved altering the executable's icon to resemble other file types and using decoy documents to make users believe they had opened a legitimate file. All the Sysget files in this campaign communicated with a single command and control (C2) server hosted at biosnews.info. Sysget used the HTTP protocol for this communication; details of the C2 traffic can be found in the Malware Details section. Over two months, all five phishing campaigns targeted a Japanese manufacturing firm, with the final campaign also targeting a separate Japanese high-tech organization.

Malware Details

In this campaign, Sysget samples were attached to emails and used various icons to deceive users into infecting their systems. Most of these samples are self-extracting executables that contain both a malicious downloader and a legitimate file. When the self-extracting executable is launched, it typically drops the downloader and the legitimate file into one of the following directories and then executes them:

- %PROGRAMFILES%
- %WINDIR%\Temp

Upon execution, the malicious downloader creates the 'mcsong[]' event to ensure only one instance is running. It then launches a new instance of 'C:\\windows\\system32\\cmd.exe' with a window name of 'Chrome-Update'. The downloader attempts to obtain a handle to this window using the FindWindowW API call and then sends a command to this executable, allowing the malware to indirectly execute a command within the cmd.exe process.

Campaign Via PlugX

This version of PlugX, a backdoor commonly utilized in targeted attacks, endeavors to conceal its presence by masquerading as a Symantec product. The sample includes an icon resembling that of Symantec.

Upon execution, the malware will install itself as a service with the following parameters:

Service Name	RasTls
Service Display Name	RasTls
Service Description	Symantec 802.1x Supplicant

Malware Details

Campaign Via FormerFirstRAT

The authors of this remote administration tool (RAT) have dubbed it "FormerFirstRAT". It communicates via unencrypted HTTP on port 443, a tactic often observed in targeted attack campaigns. Such discrepancies in ports and communication protocols can serve as indicators of malicious activity.

- The malware then proceeds to send an HTTP POST request with information about the victim system. The following information is collected:

- Victim IP address
- Username
- Administrative privileges
- RAT status (active/sleep)
- RAT version (in this case, 0.8)
- Microsoft Windows version
- UserID (Volume Serial followed by an underscore and a series of '1's)
- Language

Campaign Via NFlog

Upon being loaded into a running process, NFlog initiates by creating a new thread. This thread handles all malicious operations conducted by the DLL. Initially, the malware establishes the following registry key:

Indicator of compromise

SHA-256

1C0CF69BCE6FB6EC59BE3044D35D3A130ACDDBBF9288D7BC58B7BB87C0A4FB97

FDADA5BA799BD9F5270B218CFAD543D99FDE3EB7898FD9E3EE79603B643B3C48

6DC98A3C771F9F20D099E2D64995564DD083BE9AC6ED9586A6E57C20EBD4176C

966FF912985122C2D2D778A7DD66258F380D386EA2E1E436DA769EA702B721B3

A072133A68891A37076CD1EAF1ABB1B0BF9443488D4C6B9530E490F246008DBA

D1C7EE415A9D28F3794B8B7F768A23654491FDDD9D77C3430D33F8B6CD4C0997

1C0CF69BCE6FB6EC59BE3044D35D3A130ACDDBBF9288D7BC58B7BB87C0A4FB97

FDADA5BA799BD9F5270B218CFAD543D99FDE3EB7898FD9E3EE79603B643B3C48

6DC98A3C771F9F20D099E2D64995564DD083BE9AC6ED9586A6E57C20EBD4176C

966FF912985122C2D2D778A7DD66258F380D386EA2E1E436DA769EA702B721B3

A072133A68891A37076CD1EAF1ABB1B0BF9443488D4C6B9530E490F246008DBA

D1C7EE415A9D28F3794B8B7F768A23654491FDDD9D77C3430D33F8B6CD4C0997

HOSTNAME

freewula.strangled.net

szuunet.strangled.net

final.staticd.dynamic-dns.net

dhsg123.jkub.com

greenhugeman.dns04.com

gfsg.chickenkiller.com

pic.farisrezky.com

freewula.strangled.net

Indicator of compromise

Remediation

1. Patch Management: Regularly update software to fix vulnerabilities.
2. Network Segmentation: Limit lateral movement in case of breach.
3. User Education: Train employees to recognize threats.
4. Network Monitoring: Detect and respond to suspicious activities.
5. Incident Response Plan: Have a plan to react swiftly to breaches.
6. Application Whitelisting: Allow only approved applications.
7. Secure Remote Access: Use MFA and VPNs.
8. Threat Intelligence Sharing: Stay informed about emerging threats.
9. Security Audits: Regularly test systems for vulnerabilities.
10. Backup and Recovery: Back up data regularly and securely.
11. Block all IOCs on your XDR, EDR and other security tools.


THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE
Cyber Threat Advisory
Secure your byte world
+1 (832) 271 2738
info@threatcure.net
https://threatcure.net/