ADVISORY FOR ICM SECTORS

“Stayin’ Alive” Campaign Employed Spear-Phishing Techniques

Original report published on: October 11, 2023[1]

Executive Summary

Check Point Research disclosed a campaign named “Stayin’ Alive” targeting telecommunications industry and government organisations in Asia since 2021. The primary motivation behind this campaign is intelligence gathering and utilising a range of loaders and downloaders to extract data.

“Stayin’ Alive” campaign employed spear-phishing emails to deliver archive files. The archive files are designed to take advantage of CVE-2022-23748[2], a 7.8 high criticality Dynamic-Link Library (DLL) sideloading vulnerability to drop loaders and downloaders onto target devices.

The threat actors behind the “Stayin’ Alive” campaign utilise multiple unique loaders and downloaders, all connected to the same set of infrastructure, linked to a Chinese affiliated threat actor that most referred to as “ToddyCat.”

Background

The loaders and downloaders utilised in this campaign vary widely and have relatively basic functionality. Despite their basic nature, these deployed executables/tools prove sufficient for attackers to acquire information about the compromised machines. This suggests that the tools used are disposable, which makes detection and attribution efforts more difficult.

To defend against this campaign, Check Point Research recommends a layered approach, the first being having proper email protection to identify malicious attachment. Another level is endpoint detection and response (EDR) endpoints, to identify the DLL sideloading and malicious shell activity.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Refer to the MITRE ATT&CK techniques in this advisory:
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.
- Regularly monitor the attack surface and examine any unusual activities that could signal the lateral movement of a threat actor or the presence of malware.
- Use encryption and authentication methods to protect your data.
- Validate before adding malicious file hashes to blocklist in anti-virus and/or EDR and eXtended Detection and Response (XDR).
- Closely monitor inbound and outbound network traffic for suspicious communications or data transmissions

IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess their potential impact prior to deploying defensive measures.

Indicators of Compromise[1]

SHA256 Hash	Description
6eaa3381236586551204402 0bc4b95079a1cc2ddc26cdadf24a9ff76c81b1746	CurLu
78faceaf9a911d966086071ff085f2d5c2713b58446d48e0db1ad40974bb15cd	CurLu
295b99219d8529d2cd17b71a7947d370809f4e1a3094a74a31da6e30aa39e719	CurKeep Payload
409948cbbeaf051a41385d2e2bc32fc1e59789986852e608124b201d079e5c3c	CurLog
462c85f6972da64af08f52a4c2f3a03bcd40fdf29b29b01631bff643cd9d906a	CurKeep Payload
4d52d40bc7599b784a86a000ff436527babc46c5de737e19ded265416b4977c6	CurLu
437cde10797b75ea92b1b68eb887972fe43b434db3ed67b756e01698cce69b4a	CurKeep Archive
c5d1ee44ec75fc31e1c11fbf7a70ed7ca8c782099abfde15ecaa1b1edaf180ac	CurLog
da2d9ed632576eca68a0c6d8d5afd383a1d811c369012f0d7fb52cd06da8c9b9	CurLu
451f87134438fa7e5735a865989072e7bab4858ca0b1e921224ed27dea0226b0	CurCore
93e9237afaff14c6b9a24cf7275e9d66bc95af8a0cc93db2a68b47cbbca4c347	CurLu
482d41c4a2e14ddc072087a1b96f6e34ffda2bfc85819e21f15c97220825e651	CurKeep
877579185a72fbaf1afa78d3c50dbab187780d545d5375ba4c29147083176697	CurKeep Archive
c4f9bc7624509190e9e2a690daeff5ac9e944f094b51781734b83a364ae038d0	CurLog
d94ed414dbfb9bbcba42e3bf2db3b76eb8172b03133d1745d6abcde6f9edbaa7	CurCore
732621aa53683c16edf3959dfe9d93de5359c431c130784b31d4a598fbbd80a9	Old Vietnam Mscoree
12a7b9fa57719109b7f5d081cbe032320a59a7d57eef2dcd2cd4fe2b909162dc	CurLu
a54e0352653146371efd727ca00110577f8e750e92101462e246f99d435b6172	CurKeep
60030b970491bced72a56c9dde09a1d2260becfbf80a2b0d217a0b913e781c3a	StylerServ
36b4a846d6ed3461e36ed9f4c03fb4548397659ef0a46219695666266eba1652	CurKeep
b3fc497f94ac04abc4c9a6f23ab142fdc2387c520ce5c6fdae1b511793bc6ba2	Old Vietnam Mscoree
caa9fdda2776f681ec294ffeded04723107cf754a2889c3fbb5bc7c743d897c1	CurKeep Payload
4baa4071a5eedbe0a8afa1059f7732e5cde0433dd0425e075721dd2cdec9d70d	CurLu

d4bd89ff56b75fc617f83eb858b6dbce7b36376889b07fa0c2417322ca361c30	CurKeep
47de9bf5f60504c229fe9f727aa59ba5c34d173a23af70822541a9e485abe391	StylerServ Configs
1428698cc8b31a2c0150065af7b615ef2374ea3438b0a82f2efcff306b43cee6	CurKeep Email
2dfba1cbc0ac1793ffd591c88024fab598a3f6a91756a2ea79f84f1601a0f1ed	CurLog Archive
d33cbdbd6181deb0e8da9c9e6fb8795e98478d9608ab187e5b8809bed6b2e5c4	CurKeep Payload
6f3de35c531993aa307729e2046ff7aa672f5058b7e0fc6557bbd4c500fb46e7	Old Vietnam
2ab1121c603b925548a823fa18193896cd24d186e08957393e6a34d697aed782	CurKeep
1934ac9067871a61958e3e96ea5daa227900b7683fce67a1bf1c24beff77d75a	CurKeep Payload
a8a026d9bda80cc9bdd778a6ea8c88edcb2d657dc481952913bbdb5f2bfc11c9	CurLu
778b2526965dc1c4bcc401d0ae92037122e7e7f2c41f042f95b59a7f0fe6f30e	CurLog
7418c4d96cb0fe41fc95c0a27d2364ac45eb749d7edbe0ab339ea954f86abf9e	CurLu

Domain	**Description**
ns01[.]nayatel[.]orinafz[.]com	Malicious Domain
eaq[.]machineaccountquota[.]com	Malicious Domain
qaq2[.]machineaccountquota[.]com	Malicious Domain
imap[.]774b884034c450b[.]com	Malicious Domain
admit[.]pkigoscorp[.]com	Malicious Domain
update[.]certexvpn[.]com	Malicious Domain
cyberguard[.]certexvpn[.]com	Malicious Domain
gist[.]gitbusercontent[.]com	Malicious Domain
git[.]gitbusercontent[.]com	Malicious Domain
raw[.]gitbusercontent[.]com	Malicious Domain
cert[.]qform3d[.]in	Malicious Domain
admit[.]pkigoscorp[.]com	Malicious Domain
sslvpn[.]pkigoscorp[.]com	Malicious Domain
cdn[.]pkigoscorp[.]com	Malicious Domain

idp[.]pkigoscorp[.]com	Malicious Domain
ad[.]fopingu[.]com	Malicious Domain
proxy[.]rtmcsync[.]com	Malicious Domain
pic[.]rtmcsync[.]com	Malicious Domain
backend[.]rtmcsync[.]com	Malicious Domain

IP	**Description**
70[.]34[.]201[.]229	Malicious IP
185[.]136[.]163[.]129	Malicious IP
45[.]77[.]171[.]170	Malicious IP
167[.]179[.]91[.]150	Malicious IP
185[.]243[.]112[.]223	Malicious IP
207[.]148[.]69[.]74	Malicious IP
139[.]180[.]145[.]121	Malicious IP
77[.]91[.]75[.]232	Malicious IP
178[.]23[.]190[.]206	Malicious IP
136[.]244[.]111[.]25	Malicious IP
185[.]242[.]85[.]124	Malicious IP
45[.]159[.]250[.]179	Malicious IP
178[.]23[.]190[.]206	Malicious IP
65[.]20[.]68[.]126	Malicious IP

MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Reconnaissance	T1592	Gather Victim Host Information
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1053.005	Scheduled Task/Job: Scheduled Task
	T1059	Command and Scripting Interpreter

Persistence	T1574.007	Hijack Execution Flow: Path Interception by PATH Environment Variable
	T1574.002	Hijack Execution Flow: DLL Side-Loading
Defence Evasion	T1027	Obfuscated Files or Information
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
Exfiltration	T1048	Exfiltration Over Alternate Protocol

References

1. ^ “STAYIN’ ALIVE – TARGETED ATTACKS AGAINST TELECOMS AND GOVERNMENT MINISTRIES IN ASIA”
2. ^ “CVE-2022-23748”