Exploiting CVE-2024-21412: A Stealer Campaign Unleashed

fortinet.com/blog/threat-research/exploiting-cve-2024-21412-stealer-campaign-unleashed

July 23, 2024

Article Contents

By Cara Lin | July 23, 2024
Affected Platforms: Microsoft Windows
Impacted Users: Microsoft Windows
Impact: The stolen information can be used for future attack
Severity Level: High

CVE-2024-21412 is a security bypass vulnerability in Microsoft Windows SmartScreen that arises from an error in handling maliciously crafted files. A remote attacker can exploit this flaw to bypass the SmartScreen security warning dialog and deliver malicious files. Over the

past year, several attackers, including Water Hydra, Lumma Stealer, and Meduza Stealer, have exploited this vulnerability.

FortiGuard Labs has observed a stealer campaign spreading multiple files that exploit CVE-2024-21412 to download malicious executable files. Initially, attackers lure victims into clicking a crafted link to a URL file designed to download an LNK file. The LNK file then downloads an executable file containing an HTA script. Once executed, the script decodes and decrypts PowerShell code to retrieve the final URLs, decoy PDF files, and a malicious shell code injector. These files aim to inject the final stealer into legitimate processes, initiating malicious activities and sending the stolen data back to a C2 server.

The threat actors have designed different injectors to evade detection and use various PDF files to target specific regions, including North America, Spain, and Thailand. This article elaborates on how these files are constructed and how the injector works.

Figure 1: Telemetry

Figure 2: Attack chain

Initial Access

To start, the attacker constructs a malicious link to a remote server to search for a URL file with the following content:

Figure 3: URL files
The target LNK file employs the “forfiles” command to invoke PowerShell, then executes “mshta” to fetch an execution file from the remote server “hxxps://21centuryart.com.”

Figure 4: LNK file
During our investigation, we collected several LNK files that all download similar executables containing an HTA script embedded within the overlay. This HTA script has set WINDOWSTATE=”minimize” and SHOWTASKBAR=”no.” It plays a crucial role in the infection chain by executing additional malicious code and seamlessly facilitating the next stages of the attack.

Figure 5: HTA script in overlay
After decoding and decrypting the script, a PowerShell code downloads two files to the “%AppData%” folder. The first is a decoy PDF, a clean file that extracts the victim’s attention from malicious activity, and the other is an execution file that injects shell code for the next stage.

Figure 1: Telemetry

Figure 7: Decoy PDF files

Shell Code Injector

In this attack chain, we identified two types of injectors. The first leverages an image file to obtain a shell code. As of mid-July, it had low detection rates on VirusTotal.

Figure 8: Shell code injector on VirusTotal
After anti-debugging checking, it starts downloading a JPG file from the Imghippo website, “hxxps://i.imghippo[.]com/files/0hVAM1719847927[.]png.” It then uses the Windows API “GdipBitmapGetPixel” to access the pixels and decode the bytes to get the shell code.

Figure 9: Getting the PNG file
It then calls “dword ptr ss:[ebp-F4]” to the entry point of the shell code. The shell code first obtains all the APIs from a CRC32 hash, creates a folder, and drops files in “%TEMP%.” We can tell that these dropped files are HijackLoader based on the typical bytes “\x49\x44\x41\x54\xC6\xA5\x79\xEA” found in the encrypted data.

Figure 10: Call shell code's entry point

Figure 11: CRC32 hashes for Windows APIs

Figure 12: Dropping files in the temp folder

Figure 13: Dropped HijackLoader files
The other injector is more straightforward. It decrypts its code from the data section and uses a series of Windows API functions—NtCreateSection, NtMapViewOfSection, NtUnmapViewOfSection, NtMapViewOfSection again, and NtProtectVirtualMemory—to perform shell code injection.

Figure 14: Assembly code for calling shell code

Final Stealers

This attack uses Meduza Stealer version 2.9 and the panel found at hxxp://5[.]42[.]107[.]78/auth/login.

Figure 15: Meduza Stealer's panel
We also identified an ACR stealer loaded from HijackLoader. This ACR stealer hides its C2 with a dead drop resolver (DDR) technique on the Steam community website, hxxps://steamcommunity[.]com/profiles/76561199679420718.

Figure 16: Base64 encoded C2 on Steam
We also found the C2 for other ACR Stealers on Steam by searching for the specific string, “t6t”.

Figure 17: Other ACR Stealer’s C2 server information on Steam

After retrieving the C2 hostname, the ACR stealer appends specific strings to construct a complete URL, “hxxps://pcvcf[.]xyz/ujs/a4347708-adfb-411c-8f57-c2c166fcbe1d”. This URL then fetches the encoded configuration from the remote server. The configuration data typically contains crucial information, such as target specifics and operational parameters for the stealer. By decoding the C2 from Steam, the stealer can adapt legitimate web services to maintain communications with its C2 server.

Figure 18: Decoded ACR Stealer's configuration
Except for local text files in paths “Documents” and “Recent, “ ACR Stealer has the following target applications:

- **Browser:** Google Chrome, Google Chrome SxS, Google Chrome Beta, Google Chrome Dev, Google Chrome Unstable, Google Chrome Canary, Epic Privacy Browser, Vivaldi, 360Browser Browser, CocCoc Browser, K-Melon, Orbitum, Torch, CentBrowser, Chromium, Chedot, Kometa, Uran, liebao, QIP Surf, Nichrome, Chromodo, Coowon, CatalinaGroup Citrio, uCozMedia Uran, Elements Browser, MapleStudio ChromePlus, Maxthon3, Amigo, Brave-Browser, Microsoft Edge, Opera Stable, Opera GX Stable, Opera Neon, Mozilla Firefox, BlackHawk, and TorBro.
- **CryptoWallet:** Bitcoin, Binance, Electrum, Electrum-LTC, Ethereum, Exodus, Anoncoin, BBQCoin, devcoin, digitalcoin, Florincoin, Franko, Freicoin, GoldCoin (GLD), GInfinitecoin, IOCoin, Ixcoin, Litecoin, Megacoin, Mincoin, Namecoin, Primecoin, Terracoin, YACoin, Dogecoin, ElectronCash, MultiDoge, com.liberty.jaxx, atomic, Daedalus Mainnet, Coinomi, Ledger Live, Authy Desktop, Armory, DashCore, Zcash, Guarda, WalletWasabi, and Monero.
- **Messenger:** Telegram, Pidgin, Signal, Tox, Psi, Psi+, and WhatsApp.
- **FTP Client:** FileZilla, GoFTP, UltraFXP, NetDrive, FTP Now, DeluxeFTP, FTPGetter, Steed, Estsoft ALFTP, BitKinex, Notepad++ plugins NppFTP, FTPBox, INSoftware NovaFTP, and BlazeFtp.
- **Email Clients:** Mailbird, eM Client, The Bat!, PMAIL, Opera Mail, yMail2, TrulyMail, Pocomail, and Thunderbird.
- **VPN Service:** NordVPN and AzireVPN.
- **Password Manager:** Bitwarden, NordPass, 1Password, and RoboForm.
- **Other:** AnyDesk, MySQL Workbench, GHISLER, Sticky Notes, Notezilla , To-Do DeskList, snowflake-ssh, and GmailNotifierPro.
- **The following Chrome Extensions:**

nphplpgoakhhjchkkhmiggakijnkhfnd	apbldaphppcdfbdnnogdikheafliigcf
fldfpgipfncgndfolcbkdeeknbbbnhcc	ckdjpkejmlgmanmmdfeimelghmdfeobe
omaabbefbmiijedngplfjmnooppbclkk	iodngkohgeogpicpibpnaofoeifknfdo

afbcbjpbpfadlkmhmclhkeeodmamcflc	hnefghmjgbmpkjjfhefnenfnejdjneog
lodccjjbdhfakaekdiahmedfbieldgik	fpcamiejgfmmhnhbcafmnefbijblinff
hcflpincpppdclinealmandijcmnkbgn	egdddjbjlcjckiejbbaneobkpgnmpknp
bcopgchhojmggmffilplmbdicgaihlkp	nihlebdlccjjdejgocpogfpheakkpodb
fhmfendgdocmcbmfikdcogofphimnkno	ilbibkgkmlkhgnpgflcjdfefbkpehoom
kpfopkelmapcoipemfendmdcghnegimn	oiaanamcepbccmdfckijjolhlkfocbgj
fhbohimaelbohpjbbldcngcnapndodjp	ldpmmllpgnfdjkmhcficcifgoeopnodc
cnmamaachppnkjgnildpdmkaakejnhae	mbcafoimmibpjgdjboacfhkijdkmjocd
nlbmnnijcnlegkjjpcfjclmcfggfefdm	jbdpelninpfbopdfbppfopcmoepikkgk
amkmjjmmflddogmhpjloimipbofnfjih	onapnnfmpjmbmdciplljnjmjdjfonfjdm
cphhlgmgameodnhkjdmkpanlelnlohao	cfdldlejlcgbgollnbonjgladpgeogab
kncchdigobghenbbaddojjnnaogfppfj	ablbagjepecncofimgjmdpnhnfjiecfm
jojhfeoedkpkglbfimdfabpdfjaoolaf	fdfigkbdjmhpdgffnbdbicdmimfikfig
ffnbelfdoeiohenkjibnmadjiehjhajb	njojblnpemjkgkchnpbfllpofaphbokk
pdgbckgdncnhihllonhnjbdoighgpimk	hjagdglgahihloifacmhaigjnkobnnih
ookjlbkiijinhpmnjffcofjonbfbgaoc	pnlccmojcmeohlpggmfnbbiapkmbliob
mnfifefkajgofkcjkemidiaecocnkjeh	ljfpcifpgbbchoddpjefaipoiigpdmag
flpiciilemghbmfalicajoolhkkenfel	bhghoamapcdpbohphigoooaddinpkbai

jfdlamikmbghhapbgfoogdffldioobgl	gaedmjdfmmahhbjefcbgaolhhanlaolb
nkbihfbeogaeaoehlefnkodbefgpgknn	imloifkgjagghnncjkhggdhalmcnfklk
aiifbnbfobpmeekipheeijimdpnlpgpp	oeljdldpnmdbchonielidgobddfffflal
aeachknmefphepccionboohckonoeemg	ilgcnhelpchnceeipipijaljkblbcobl
hpglfhgfnhbgpjdenjgmdgoeiappafln	nngceckbapebfimnlniiiahkandclblb
nknhiehlklippafakaeklbeglecifhad	oboonakemofpalcgghocfoadofidjkkk
dmkamcknogkgcdfhhbddcghachkejeap	fdjamakpfbbddfjaooikfcpapjohcfmg
jnmbobjmhlngoefaiojfljckilhhlhcj	fooolghllnmhmmndgjiamiiodkpenpbb
klnaejjgbibmhlephnhpmaofohgkpgkd	bfogiafebfohielmmehodmfbbebbbpei
ibnejdfjmmkpcnlpebklmnkoeoihofec	lfochlioelphaglamdcakfjemolpichk
ejbalbakoplchlghecdalmeeeajnimhm	hdokiejnpimakedhajhdlcegeplioahd
kjmoohlgokccodicjjfebfomlbljgfhk	naepdomgkenhinolocfifgehidddafch
fnjhmkhhmkbjkkabndcnnogagogbneec	bmikpgodpkclnkgmnpphehdgcimmided
nhnkbkgjikgcigadomkphalanndcapjk	nofkfblpeailgignhkbnapbephdnmbmn
hnfanknocfeofbddgcijnmhnfnkdnaad	jhfjfclepacoldmjmkmdlmganfaalklb
cihmoadaighcejopammfbmddcmdekcje	chgfefjpcobfbnpmiokfjjaglahmnded
bfnaelmomeimhlpmgjnjophhpkkoljpa	igkpcodhieompeloncfnbekccinhapdb
djclckkglechooblngghdinmeemkbgci	cfhdojbkjhnklbpkdaibdccddilifddb

jiidiaalihmmhddjgbnbgdfflelocpak	kmmkllgcgpldbblpnhghdojehhfafhro
lgmpcpglpngdoalbgeoldeajfclnhafa	ibegklajigjlbljkhfpenpfoadebkokl
egjidjbpglichdcondbcbdnbeeppgdph	ijpdbdidkomoophdnnnfoancpbbmpfcn
flhbololhdbnkpnnocoifnopcapiekdi	llalnijpibhkmpdamakhgmcagghgmjab
kkhmbjifakpikpapdiaepgkdephjgnma	mjdmgoiobnbombmnbbdllfncjcmopfnc
ekkhlihjnlmjenikbgmhgjkknoelfped	dlcobpjiigpikoobohmabehhmhfoodbb
jngbikilcgcnfdbmnmnmnleeomffciml	jnlgamecbpmbajjfhmmmlhejkemejdma
hcjginnbdlkdnnahogchmeidnmfckjom	kbdcddcmgoplfockflacnnefaehaiocb
ogphgbfmhodmnmpnaadpbdadldbnmjji	kgdijkcfiglijhaglibaidbipiejjfdp
hhmkpbimapjpajpicehcnmhdgagpfmjc	epapihdplajcdnnkdeiahlgigofloibg
ojhpaddibjnpiefjkbhkfiaedepjheca	mgffkfbidihjpoaomajlbgchddlicgpn
fmhjnpmdlhokfidldlglfhkkfhjdmhgl	ebfidpplhabeedpnhjnobghokpiioolj
gjhohodkpobnogbepojmopnaninookhj	dngmlblcodfobpdpecaadgfbcggfjfnm
hmglflngjlhgibbmcedpdabjmcmboamo	ldinpeekobnhjjdofggfgjlcehhmanlj
eklfjjkfpbnioclagjlmklgkcfmgmbpg	mdjmfdffdcmnoblignmgpommbefadffd
jbkfoedolllekgbhcbcoahefnbanhhlh	aflkmfhebedbjioipglgcbcmnbpgliof
mcohilncbfahbmgdjkbpemcciiolgcge	dmjmllblpcbmniokccdoaiahcdajdjof
jbdaocneiiinmjbjlgalhcelgbejmnid	lnnnmfcpbkafcpgdilckhmhbkkbpkmid

blnieiiffboillknjnepogjhkgnoapac	odpnjmimokcmjgojhnhfcnalnegdjmdn
cjelfplplebdjjenllpjcblmjkfcffne	bopcbmipnjdcdfflfgjdgdjejmgpoaab
fihkakfobkmkjojpchpfgcmhfjnmnfpi	cpmkedoipcpimgecpmgpldfpohjplkpp
kkpllkodjeloidieedojogacfhpaihoh	khpkpbbcccdmmclmpigdgddabeilkdpd
nanjmdknhkinifnkgdcggcfnhdaammmj	mcbigmjiafegjnnogedioegffbooigli
nkddgncdjgjfcddamfgcmfnlhccnimig	fiikommddbeccaoicoejoniammnalkfa
acmacodkjbdgmoleebolmdjonilkdbch	heefohaffomkkkphnlpohglngmbcclhi
phkbamefinggmakgklpkljjmgibohnba	ocjdpmoallmgmjbbogfiiaofphbjgchh
efbglgofoippbgcjepnhiblaibcnclgk	hmeobnfnfcmdkdcmlblgagmfpfboieaf
lpfcbjknijpeeillifnkikgncikgfhdo	kfdniefadaanbjodldohaedphafoffoh
ejjladinnckdgjemekebdpeokbikhfci	kmhcihpebfmpgmihbkipmjlmmioameka
opcgpfmipidbgpenhmajoajpbobppdil	gafhhkghbfjjkeiendhlofajokpaflmk
aholpfdialjgjfhomihkjbmgjidlcdno	kglcipoddmbniebnibibkghfijekllbl
onhogfjeacnfoofkfgppdlbmlmnplgbn	iokeahhehimjnekafflcihljlcjccdbe
mopnmbcafieddcagagdcbnhejhlodfdd	idnnbdplmphpflfnlkomgpfbpcgelopg
fijngjgcjhjmmpcmkeiomlglpeiijkld	kmphdnilpmdejikjdnlbcnmnabepfgkh
hifafgmccdpekplomjjkcfgodnhcellj	cgeeodpfagjceefieflmdfphplkenlfk
ijmpgkjfkbfhoebgogflfebnmejmfbm	pdadjkfkgcafgbceimcpbkalnfnepbnk

lkcjlnjfpbikmcmbachjpdbijejflpcm	odbfpeeihdkbihmopkbjmoonfanlbfcl
onofpnbbkehpmmoabgpcpmigafmmnjh	fhilaheimglignddkjgofkcbgekhenbh
dkdedlpgdmmkkfjabffeganieamfklkm	aodkkagnadcbobfpggfnjeongemjbjca
nlgbhdfgdhgbiamfdfmbikcdghidoadd	dngmlblcodfobpdpecaadgfbcggfjfnm
infeboajgfhgbjpjbeppbkgnabfdkdaf	lpilbniiabackdjcionkobglmddfbcjo
ppbibelpcjmhbdihakflkdcoccbgbkpo	bhhhlbepdkbapadjdnnojkbgioiodbic
klghhnkeealcohjjanjjdaeeggmfmlpl	jnkelfanjkeadonecabehalmbgpfodjm
enabgbdfcbaehmbigakijjabdpdnimlg	jgaaimajipbpdogpdglhaphldakikgef
mmmjbcfofconkannjonfmjjajplldbg	kppfdiipphfccemcignhifpjkapfbihd
bifidjkcdpgfnlbcjpdkdcnbiooooblg	loinekcabhlmhjjbocijdoimmejangoa
nebnhfamliijlghikdgcigoebonmoibm	anokgmphncpekkhclmingpimjmcooifb
fcfcfllfndlomdhbehjjcoimbgofdncg	cnncmdhjacpkmjmkcafchppbnpnhdmon
ojggmchlghnjlapmfbnjholfjkiidbch	mkpegjkblkkefacfnmkajcjmabijhclg

Conclusion

This campaign primarily targets CVE-2024-21412 to spread LNK files for downloading execution files that embed HTA script code within their overlays. The HTA script runs silently, avoiding any pop-up windows, and clandestinely downloads two files: a decoy PDF and an execution file designed to inject shell code, setting the stage for the final stealers.

To mitigate such threats, organizations must educate their users about the dangers of downloading and running files from unverified sources. Continuous innovation by threat actors necessitates a robust and proactive cybersecurity strategy to protect against sophisticated attack vectors. Proactive measures, user awareness, and stringent security protocols are vital components in safeguarding an organization's digital assets.

Fortinet Protections

The malware described in this report is detected and blocked by FortiGuard Antivirus:

LNK/Agent.OQ!tr
LNK/Agent.BNE!tr
LNK/Agent.ACX!tr
W32/Agent.DAT!tr
W64/Agent.EDE6!tr
W32/Agent.AAN!tr
W64/Agent.A8D2!tr

FortiGate, FortiMail, FortiClient, and FortiEDR support the FortiGuard AntiVirus service. The FortiGuard AntiVirus engine is part of each of these solutions. As a result, customers who have these products with up-to-date protections are protected.

The FortiGuard Web Filtering Service blocks the C2 servers and downloads URLs.

FortiGuard Labs provides IPS signature against attacks exploiting CVE-2024-21412:

MS.Windows.SmartScreen.CVE-2024-21412.Security.Feature.Bypass

We also suggest that organizations go through Fortinet's free NSE training module: NSE 1 – Information Security Awareness. This module is designed to help end users learn how to identify and protect themselves from phishing attacks.

FortiGuard IP Reputation and Anti-Botnet Security Service proactively block these attacks by aggregating malicious source IP data from the Fortinet distributed network of threat sensors, CERTs, MITRE, cooperative competitors, and other global sources that collaborate to provide up-to-date threat intelligence about hostile sources.

If you believe this or any other cybersecurity threat has impacted your organization, please contact our Global FortiGuard Incident Response Team.

IOCs

IP Addresses

62[.]133[.]61[.]26

62[.]133[.]61[.]43

5[.]42[.]107[.]78

Hostnames

21centuryart[.]com

scratchedcards[.]com

proffyrobharborye[.]xyz

answerrsdo[.]shop

pcvcf[.]xyz

pcvvf[.]xyz

pdddk[.]xyz

pdddj[.]xyz

pddbj[.]xyz

pbpbj[.]xyz

pbdbj[.]xyz

ptdrf[.]xyz

pqdrf[.]xyz

Files

e15b200048fdddaedb24a84e99d6d7b950be020692c02b46902bf5af8fb50949

547b6e08b0142b4f8d024bac78eb1ff399198a8d8505ce365b352e181fc4a544

bd823f525c128149d70f633e524a06a0c5dc1ca14dd56ca7d2a8404e5a573078

982338768465b79cc8acd873a1be2793fccbaa4f28933bcdf56b1d8aa6919b47

bc6933a8fc324b907e6cf3ded3f76adc27a6ad2445b4f5db1723ac3ec86ed10d

59d2c2ca389ab1ba1fefa4a06b14ae18a8f5b70644158d5ec4fb7a7eac4c0a08

8568226767ac2748eccc7b9832fac33e8aa6bfdc03eafa6a34fb5d81e5992497

4043aa37b5ba577dd99f6ca35c644246094f4f579415652895e6750fb9823bd9

0604e7f0b4f7790053991c33359ad427c9bf74c62bec3e2d16984956d0fb9c19

8c6d355a987bb09307e0af6ac8c3373c1c4cbfbceeeb1159a96a75f19230ede6

de6960d51247844587a21cc0685276f966747e324eb444e6e975b0791556f34f

6c779e427b8d861896eacdeb812f9f388ebd43f587c84a243c7dab9ef65d151c

08c75c6a9582d49ea3fe780509b6f0c9371cfcd0be130bc561fae658b055a671

abc54ff9f6823359071d755b151233c08bc2ed1996148ac61cfb99c7e8392bfe

643dde3f461907a94f145b3cd8fe37dbad63aec85a4e5ed759fe843b9214a8d2