Threat Intelligence

Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser

October 28, 2020

Mandiant

Written by: Kimberly Goody, Jeremy Kennelly, Joshua Shilko, Steve Elovitz, Douglas Bienstock

Throughout 2020, ransomware activity has become increasingly prolific, relying on an ecosystem of distinct but co-enabling operations to gain access to targets of interest before conducting extortion. Mandiant Threat Intelligence has tracked several loader and backdoor campaigns that lead to the post-compromise deployment of ransomware, sometimes within 24 hours of initial compromise. Effective and fast detection of these campaigns is key to mitigating this threat.

The malware families enabling these attacks previously reported by Mandiant to intelligence subscribers include KEGTAP/BEERBOT, SINGLEMALT/STILLBOT and WINEKEY/CORKBOT. While these malware families communicate with the same command and control infrastructure (C2) and are close to functional parity, there are minimal code overlaps across them. Other security researchers have tracked these malware families under the names BazarLoader and BazarBackdoor or Team9.

The operators conducting these campaigns have actively targeted hospitals, retirement communities, and medical centers, even in the midst of a global health crisis, demonstrating a clear disregard for human life.

Email Campaign TTPs

Campaigns distributing KEGTAP, SINGLEMALT and WINEKEY have been

and procedures (TTPs). Despite the frequent changes seen across these campaigns, the following has remained consistent across recent activity:

- Emails contain an in-line link to an actor-controlled Google Docs document, typically a PDF file.
- This document contains an in-line link to a URL hosting a malware payload.
- Emails masquerade as generic corporate communications, including follow-ups about documents and phone calls or emails crafted to appear related to complaints, terminations, bonuses, contracts, working schedules, surveys or queries about business hours.
- Some email communications have included the recipient's name or employer name in the subject line and/or email body.

Despite this uniformity, the associated TTPs have otherwise changed regularly—both between campaigns and across multiple spam runs seen in the same day. Notable ways that these campaigns have varied over time include:

- Early campaigns were delivered via Sendgrid and included in-line links to Sendgrid URLs that would redirect users to attacker-created Google documents. In contrast, recent campaigns have been delivered via attacker-controlled or compromised email infrastructure and have commonly contained in-line links to attacker-created Google documents, although they have also used links associated with the Constant Contact service.
- The documents loaded by these in-line links are crafted to appear somewhat relevant to the theme of the email campaign and contain additional links along with instructions directing users to click on them. When clicked, these links download malware binaries with file names masquerading as document files. Across earlier campaigns these malware binaries were hosted on compromised infrastructure, however, the attackers have shifted to hosting their malware on legitimate web services, including Google Drive, Basecamp, Slack, Trello, Yougile, and JetBrains.
- In recent campaigns, the malware payloads have been hosted on numerous URLs associated with one or more of these legitimate services. In cases where the payloads have been taken down, the actors have sometimes updated their Google documents to contain new, working links.
- Some campaigns have also incorporated customization, including emails with internal references to the recipients' organizations (Figure 1) and organizations' logos embedded into the Google Docs documents (Figure 2).

Figure 1: Email containing internal references to target an organization's name

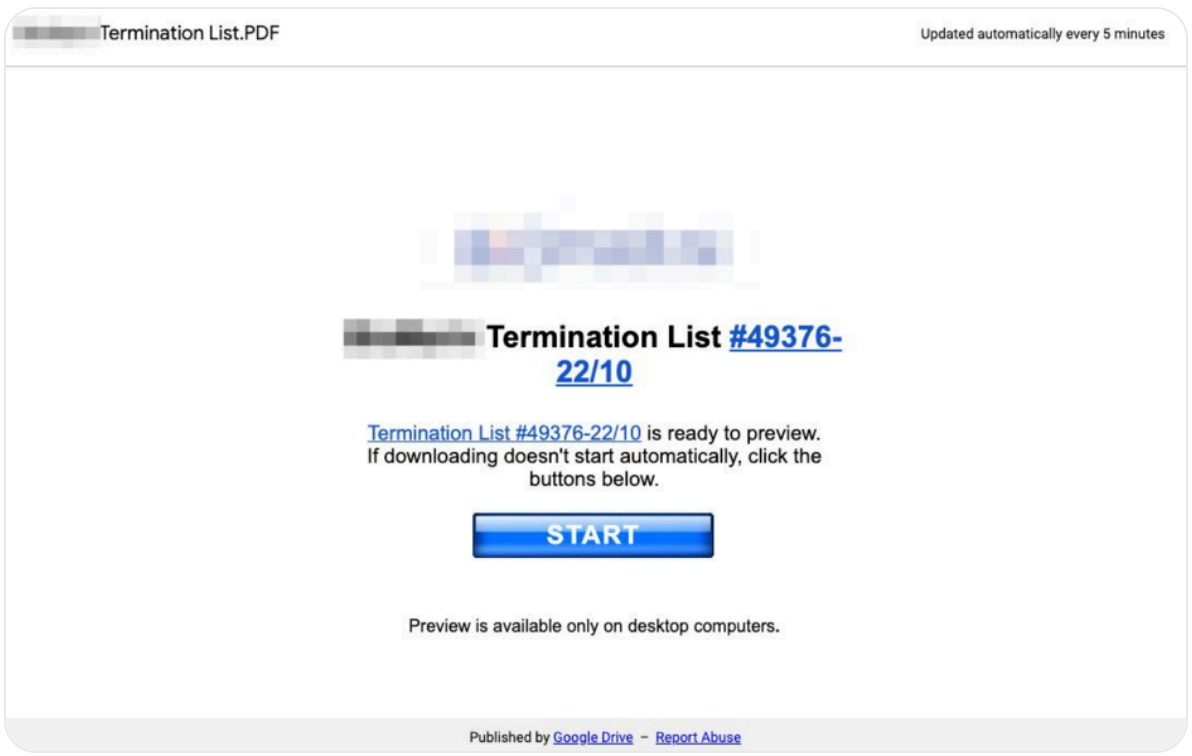

Figure 2: Google Docs PDF document containing a target organization's logo

Hiding the final payload behind multiple links is a simple yet effective way to bypass some email filtering technologies. Various technologies have the ability to follow links in an email to try to identify malware or malicious domains; however, the number of links followed can vary. Additionally, embedding links within a PDF document further makes automated detection and link-following difficult.

Post-Compromise TTPs

Given the possibility that accesses obtained from these campaigns may be provided to various operators to monetize, the latter-stage TTPs, including ransomware family deployed, may vary across intrusions. A notable majority of cases where Mandiant has had visibility into these post-compromise TTPs have been attributable to UNC1878, a financially motivated actor that monetizes network access via the deployment of RYUK ransomware.

Establish Foothold

Once the loader and backdoor have been executed on the initial victim host, the actors have used this initial backdoor to download POWERTRICK and/or Cobalt Strike BEACON payloads to establish a foothold. Notably, the respective loader and backdoor as well as POWERTRICK have typically been installed on a small number of hosts in observed incidents, suggesting these payloads may be reserved for

reconnaissance. However, BEACON is frequently found on a larger number of hosts and used throughout various stages of the attack lifecycle.

Maintain Presence

Beyond the preliminary phases of each intrusion, we have seen variations in how these attackers have maintained presence after establishing an initial foothold or moving laterally within a network. In addition to the use of common post-exploitation frameworks such as Cobalt Strike, Metasploit and EMPIRE, we have observed the use of other backdoors, including ANCHOR, that we also believe to be under control of the actors behind TrickBot.

- The loaders associated with this activity can maintain persistence through reboot by using at least four different techniques, including creating a scheduled task, adding itself to the startup folder as a shortcut, creating a scheduled Microsoft BITS job using /setnotifycmdline, and adding itself to the Userinit value under the following registry key:
  - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.
- Actors have downloaded POWERTRICK, Metasploit Meterpreter, and Cobalt Strike BEACON payloads following the initial compromise. BEACON payloads have commonly been executed after moving laterally to new hosts within the victim network. The attackers have employed Cobalt Strike payloads crafted to maintain persistence through reboot via a scheduled task on critical systems in victim environments. Notably, BEACON is the backdoor observed most frequently across these incidents.
- We have observed actors executing encoded PowerShell commands that ultimately executed instances of the PowerShell EMPIRE backdoor.
- The actors were observed using BEACON to execute PowerLurk's Register-MaliciousWmiEvent cmdlet to register WMI events used to kill processes related to security tools and utilities, including Task Manager, WireShark, TCPView, ProcDump, Process Explorer, Process Monitor, NetStat, PSLoggedOn, LogonSessions, Process Hacker, Autoruns, AutorunsSC, RegEdit, and RegShot.
- In at least once case, attackers have maintained access to a victim environment using stolen credentials to access corporate VPN infrastructure configured to require only single-factor authentication.

Escalate Privileges

The most commonly observed methods for escalating privileges in these incidents have involved the use of valid credentials. The actors used a variety of techniques for accessing credentials stored in memory or on disk to access privileged accounts.

- The actors used valid credentials obtained using MimiKatz variants to escalate privileges. We've observed Mimikatz being executed both from the file system of victim hosts and via PowerShell cmdlets executed via Cobalt Strike BEACON.
- Actors have gained access to credentials via exported copies of the *ntds.dit* Active Directory database and SYSTEM and SECURITY registry hives from a Domain Controller.
- In multiple instances, the actors have launched attacks against Kerberos, including the use of RUBEUS, the MimiKatz Kerberos module, and the Invoke-Kerberoast cmdlet.

Reconnaissance

The approaches taken to perform host and network reconnaissance across these incidents varied; however, a significant portion of observed reconnaissance activity has revolved around Activity Directory enumeration using publicly available utilities such as BLOODHOUND, SHARPHOUND or ADFind, as well as the execution of PowerShell cmdlets using Cobalt Strike BEACON.

- BEACON has been installed on a large number of systems across these intrusions and has been used to execute various reconnaissance commands including both built-in host commands and PowerShell cmdlets. Observed PowerShell cmdlets include:
  - Get-GPPPassword
  - Invoke-AllChecks
  - Invoke-BloodHound
  - Invoke-EternalBlue
  - Invoke-FileFinder
  - Invoke-HostRecon
  - Invoke-Inveigh
  - Invoke-Kerberoast
  - Invoke-LoginPrompt
  - Invoke-mimikittenz
  - Invoke-ShareFinder
  - Invoke-UserHunter
- Mandiant has observed actors using POWERTRICK to execute built-in system commands on the initial victim host, including *ipconfig*, *findstr*, and *cmd.exe*.
- The actors leveraged publicly available utilities Adfind, BLOODHOUND, SHARPHOUND, and KERBRUTE on victim networks to collect Active Directory information and credentials.
- WMIC commands have been used to perform host reconnaissance, including listing installed software, listing running processes, and identifying operating system and system architecture.
- The actors have used a batch script to ping all servers identified

- The actors used the *Nltest* command to list domain controllers.

Lateral Movement

Lateral movement was most commonly accomplished using valid credentials in combination with Cobalt Strike BEACON, RDP and SMB, or using the same backdoors used to establish a foothold in victim networks.

- The actors have regularly leveraged Cobalt Strike BEACON and Metasploit Meterpreter to move laterally within victim environments.
- The actors commonly moved laterally within victim environments using compromised accounts—both those belonging to regular users and accounts with administrative privileges. In addition to the use of common post-exploitation frameworks, lateral movement has also been achieved using WMIC commands and the Windows RDP and SMB protocols.
- The actors used the Windows *net use* command to connect to Windows admin shares to move laterally.

Complete Mission

Mandiant is directly aware of incidents involving KEGTAP that included the post-compromise deployment of RYUK ransomware. We have also observed instances where ANCHOR infections, another backdoor associated with the same actors, preceded CONTI or MAZE deployment.

- In at least one case, an executable was observed that was designed to exfiltrate files via SFTP to an attacker-controlled server.
- The actors have used Cobalt Strike BEACON to exfiltrate data created through network reconnaissance activities as well as user files.
- The actors were observed deleting their tools from victim hosts in an attempt to remove indicators of compromise.
- The actors have used their access to the victim network to deploy ransomware payloads. There is evidence to suggest that RYUK ransomware was likely deployed via PsExec, but other scripts or artifacts related to the distribution process were not available for forensic analysis.

Hunting Strategies

If an organization identifies a host with an active infection believed to be an instance of KEGTAP or a parallel malware family, the following containment actions are recommended. Note that due to the velocity of this intrusion activity, these actions should be taken in parallel.

- Isolate and perform a forensic review of any impacted systems.
- Review incoming emails to the user that owns the impacted device

- Identify the URLs used by the phishing campaign and block them using proxy or network security devices.
- Reset credentials for any user accounts associated with execution of the malware.
- Perform an enterprise wide review for lateral movement authentication from the impacted systems.
- Check authentication logs from any single-factor remote access solutions that may exist (VPN, VDI, etc) and move towards multi-factor authentication (MFA) as soon as possible.

An enterprise-wide effort should be made to identify host-based artifacts related to the execution of first-stage malware and all post-intrusion activity associated with this activity. Some baseline approaches to this have been captured as follows.

Activity associated with the KEGTAP loader can often be identified via a review of system startup folders and Userinit values under the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon registry key.

```
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\adc
```

Figure 3: Example LNK file associated with KEGTAP persistence within a system's startup folders

SINGLEMALT employs BITS to maintain persistence through reboot and can often be identified via a review of anomalous BITS jobs. SINGLEMALT uses a well-documented BITS persistence mechanism that intentionally creates a job to download a non-existent URL, which will trigger a failure event. The job is set to retry on a regular interval, thus ensuring the malware continues to run. To review the BITS job on a host run the command bitsadmin /list.

- Display name may be "Adobe Update", "System autoupdate" or another generic value.
- Notify state may be set to Fail (Status 2).
- FileList URL value may be set to the local host or a URL that does not exist.
- The Notification Command Line value may contain the path to the SINGLEMALT sample and/or a command to move it to a new location then start it.
- The Retry Delay value will be set.

WINEKEY maintains persistence through reboot via the use of registry RUN keys. Searching for anomalous RUN keys enterprise-wide can help to identify systems impacted by this malware.

```
Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Bac
```

Figure 4: Example registry RUN key used by WINEKEY to maintain persistence

The ANCHOR backdoor has been seen across a subset of intrusions associated with this activity and can often be identified via the scheduled tasks it uses to maintain persistence through reboot. The scheduled tasks created by ANCHOR are often unnamed, although that is not always the case.

- The identification of named scheduled tasks associated with ANCHOR persistence may be constructed according to the following pattern: <*Random directory within %APPDATA%*> autoupdate#<*random number*>.
- All unnamed scheduled tasks should be reviewed, particularly those with a creation date consistent with the time of the suspected compromise.

Although it is a low fidelity indicator, ANCHOR activity may also sometimes be identified by searching for binaries within the C:\Windows\SysWOW64 directory that have a file name matching the following pattern: <*8 random lowercase chars*>.exe. Stacking or sorting on file creation timestamps in the C:\Windows\SysWOW64 directory may also help identify malicious files, as the directory should be mostly static.

Post-exploitation activity associated with the deployment of ransomware following these campaigns is typically conducted using the Cobalt Strike attack framework. The BEACON payload associated with Cobalt Strike can often be identified via a review of existing registered services and service creation events (Event ID 7045), both markers of the mechanism it most commonly employs to maintain persistence.

The following are additional strategies that may aid in identifying associated activity:

- Organizations can review web proxy logs in order to identify HXXP requests for file storage, project management, collaboration or communication services with a referrer from a Google Docs document.
- During the associated post-compromise activity, attackers have commonly staged their tools and data in the PerfLogs directory and C$ share.
- While collecting data used to enable later-stage operations, the attackers commonly leave instances of ntds.dit and exports of the SYSTEM and SECURITY registry hives on impacted systems.

Hardening Strategies

The actions taken by the actors to escalate privileges and move laterally in an environment use well-documented techniques that search the network and Active Directory for common misconfigurations that expose credentials and systems for abuse. Organizations can take

more in-depth recommendations see our ransomware protection white paper.

- Harden service accounts against brute force and password guessing attacks. Most organizations have at least a few service accounts with passwords set to never expire. These passwords are likely old and insecure. Make a best effort to reset as many of these accounts as possible to long and complex passwords. In cases where it is possible, migrate to MSAs and gMSAS for automated rotation.
- Prevent the usage of privileged accounts for lateral movement. Use GPOs to restrict the ability for privileged accounts such as Domain Administrators and privileged service accounts from initiating RDP connections and network logins.Actors often pick just a few accounts to use for RDP; by limiting the number of potential accounts, you provide detection opportunities and opportunities to slow the actor.
- Block internet access for servers where possible. Often times there is no business need for servers, especially AD infrastructure systems, to access the Internet. The actors often choose high-uptime servers for the deployment of post-exploitation tools such as BEACON.
- Block uncategorized and newly registered domains using web proxies or DNS filters. Often the final payload delivered via phishing is hosted on a compromised third-party website that do not have a business categorization.
- Ensure that critical patches are installed on Windows systems as well as network infrastructure. We have observed attackers exploiting well-known vulnerabilities such as Zerologon (CVE-2020-1472) to escalate privileges in an environment prior to deploying ransomware. In other cases, possibly unrelated to UNC1878, we have observed threat actors gain access to an environment through vulnerable VPN infrastructure before deploying ransomware.

For more intelligence on ransomware and other threats, please register for Mandiant Advantage Free, a no-cost version of our threat intelligence platform. Check out this episode of *State of the Hack* for additional information on this threat.

Campaign Indicators

Sample Email Subjects / Patterns

- <(first|last)-name>: Important Information
- <Company Name>
- <Company Name> complaint
- <(first|last)-name>
- <(first|last)-name>

- Agreement cancellation notification
- Agreement cancellation reminder
- Agreement suspension message
- Agreement suspension notice
- Agreement suspension notification
- Agreement suspension reminder
- Arrangement cancellation message
- Arrangement cancellation notice
- Arrangement cancellation notification
- Arrangement cancellation reminder
- Arrangement suspension message
- Arrangement suspension notice
- Arrangement suspension notification
- Arrangement suspension reminder
- Contract cancellation message
- Contract cancellation notice
- Contract cancellation notification
- Contract cancellation reminder
- Contract suspension message
- Contract suspension notice
- Contract suspension notification
- Contract suspension reminder
- debit confirmation
- FW: <Name> Annual Bonus Report is Ready
- FW: Urgent: <Company Name>: A Customer Complaint Request – Prompt Action Required
- RE: <(first|last)-name>
- RE: <(first|last)-name>: Your Payslip for October
- RE: <Company Name> - my visit
- RE: <Company Name> Employee Survey
- RE: <Company Name> office
- RE: <Name> about complaint
- RE: <Name> bonus
- RE: <Name> termination list
- RE: <Name>
- RE: <Company Name> office
- RE: <(first|last)-name>
- RE: <(first|last)-name> <(first|last)-name>: complaint
- RE: <(first|last)-name>: Subpoena
- RE: <(first|last)-name>

- RE: about complaint
- RE: Adopted Filer Forms
- RE: Business hours adjustment
- RE: Business hours realignment
- RE: Business hours rearrangement
- RE: Business hours restructuring
- RE: Business schedule adjustment
- RE: Business schedule realignment
- RE: Business schedule rearrangement
- RE: Business schedule restructuring
- RE: call me
- RE: changes
- RE: complaint
- RE: Complaint in <Company Name>.
- RE: Complaint on <Name>
- RE: customer request
- RE: debit confirmation
- RE: document copy
- RE: documents list
- RE: Edgar Filer forms renovations
- RE: employee bonuses
- RE: Filer Forms adaptations
- RE: my call
- RE: New filer form types
- RE: office
- RE: our meeting
- RE: Payroll Register
- RE: report confirmation
- RE: situation
- RE: Subpoena
- RE: termination
- RE: till 2 pm
- RE: Urgent <Company Name> Employee Internal Survey
- RE: visit
- RE: what about your opinion?
- RE: what time?
- RE: why
- RE: why this debit
- RE: Working schedule adjustment
- RE: Working schedule realignment

- RE: Working schedule restructuring
- RE: Your Payslip for September

Example Malware Family MD5s

- KEGTAP
  - df00d1192451268c31c1f8568d1ff472
- BEERBOT
  - 6c6a2bfa5846fab374b2b97e65095ec9
- SINGLEMALT
  - 37aa5690094cb6d638d0f13851be4246
- STILLBOT
  - 3176c4a2755ae00f4fffe079608c7b25
- WINEKEY
  - 9301564bdd572b0773f105287d8837c4
- CORKBOT
  - 0796f1c1ea0a142fc1eb7109a44c86cb

Code Signing Certificate CNs

- ARTBUD RADOM SP Z O O
- BESPOKE SOFTWARE SOLUTIONS LIMITED
- Best Fud, OOO
- BlueMarble GmbH
- CHOO FSP, LLC
- Company Megacom SP Z O O
- ESTELLA, OOO
- EXON RENTAL SP Z O O
- Geksan LLC
- GLOBAL PARK HORIZON SP Z O O
- Infinite Programming Limited
- James LTH d.o.o.
- Logika OOO
- MADAS d.o.o.
- MUSTER PLUS SP Z O O
- NEEDCODE SP Z O O
- Nordkod LLC
- NOSOV SP Z O O
- OOO MEP
- PLAN CORP PTY LTD

- RESURS-RM OOO
- Retalit LLC
- Rumikon LLC
- SNAB-RESURS, OOO
- TARAT d.o.o.
- TES LOGISTIKA d.o.o.
- VAS CO PTY LTD
- VB CORPORATE PTY. LTD.
- VITA-DE d.o.o.

UNC1878 Indicators

A significant proportion of the post-compromise activity associated with these campaigns has involved the distribution of RYUK ransomware by a threat group tracked by Mandiant as UNC1878. As such, we are releasing indicators associated with this group.

BEACON C2s

First Seen	Domain
12/11/19	updatemanagir[.]us
12/20/19	cmdupdatewin[.]com
12/26/19	scrservallinst[.]info
1/10/20	winsystemupdate[.]com
1/11/20	jomamba[.]best
1/13/20	updatewinlsass[.]com
1/16/20	winsysteminfo[.]com
1/20/20	livecheckpointsrs[.]com
1/21/20	ciscocheckapi[.]com
1/28/20	timesshifts[.]com
1/29/20	cylenceprotect[.]com
1/30/20	sophosdefence[.]com
1/30/20	taskshedulewin[.]com

1/30/20	windefenceinfo[.]com
1/30/20	lsasswininfo[.]com
1/30/20	update-wind[.]com
1/30/20	lsassupdate[.]com
1/30/20	renovatesystem[.]com
1/31/20	updatewinsoftr[.]com
2/2/20	cleardefencewin[.]com
2/2/20	checkwinupdate[.]com
2/2/20	havesetup[.]net
2/3/20	update-wins[.]com
2/3/20	conhostservice[.]com
2/4/20	microsoftupdateswin[.]com
2/4/20	iexploreservice[.]com
2/12/20	avrenew[.]com
2/12/20	target-support[.]online
2/12/20	web-analysis[.]live
2/14/20	freeallsafe[.]com
2/17/20	windefens[.]com
2/17/20	defenswin[.]com
2/17/20	easytus[.]com
2/17/20	greattus[.]com
2/17/20	livetus[.]com
2/17/20	comssite[.]com

2/17/20	bigtus[.]com
2/17/20	aaatus[.]com
2/17/20	besttus[.]com
2/17/20	firsttus[.]com
2/17/20	worldtus[.]com
2/26/20	freeoldsafe[.]com
2/26/20	serviceupdates[.]net
2/26/20	topserviceupdater[.]com
2/27/20	myserviceupdater[.]com
2/29/20	myservicebooster[.]net
2/29/20	servicesbooster[.]org
2/29/20	brainschampions[.]com
2/29/20	myservicebooster[.]com
2/29/20	topservicesbooster[.]com
2/29/20	servicesbooster[.]com
2/29/20	topservicesecurity[.]org
2/29/20	topservicesecurity[.]net
2/29/20	topsecurityservice[.]net
2/29/20	myyserviceupdater[.]com
2/29/20	topservicesupdate[.]com
2/29/20	topservicesecurity[.]com
2/29/20	servicesecurity[.]org
2/29/20	myserviceconnect[.]net

3/2/20	yoursuperservice[.]com
3/2/20	topservicehelper[.]com
3/2/20	serviceuphelper[.]com
3/2/20	serviceshelpers[.]com
3/2/20	boostsecuritys[.]com
3/3/20	hakunamatatata[.]com
3/8/20	service-updater[.]com
3/9/20	secondserviceupdater[.]com
3/9/20	twelvethserviceupdater[.]com
3/9/20	twentiethservicehelper[.]com
3/9/20	twelfthservicehelper[.]com
3/9/20	tenthservicehelper[.]com
3/9/20	thirdserviceupdater[.]com
3/9/20	thirdservicehelper[.]com
3/9/20	tenthserviceupdater[.]com
3/9/20	thirteenthservicehelper[.]com
3/9/20	seventeenthservicehelper[.]com
3/9/20	sixteenthservicehelper[.]com
3/9/20	sixthservicehelper[.]com
3/9/20	seventhservicehelper[.]com
3/9/20	seventhserviceupdater[.]com
3/9/20	sixthserviceupdater[.]com
3/9/20	secondservicehelper[.]com

3/9/20	ninethserviceupdater[.]com
3/9/20	fourteenthservicehelper[.]com
3/9/20	fourthserviceupdater[.]com
3/9/20	firstserviceupdater[.]com
3/9/20	firstservisehelper[.]com
3/9/20	fifthserviceupdater[.]com
3/9/20	eleventhserviceupdater[.]com
3/9/20	fifthservicehelper[.]com
3/9/20	fourservicehelper[.]com
3/9/20	eighthservicehelper[.]com
3/9/20	eighteenthservicehelper[.]com
3/9/20	eighthserviceupdater[.]com
3/9/20	fifteenthservicehelper[.]com
3/9/20	nineteenthservicehelper[.]com
3/9/20	eleventhservicehelper[.]com
3/14/20	thirdservice-developer[.]com
3/14/20	fifthservice-developer[.]com
3/15/20	firstservice-developer[.]com
3/16/20	fourthservice-developer[.]com
3/16/20	ninethservice-developer[.]com
3/16/20	seventhservice-developer[.]com
3/16/20	secondservice-developer[.]com
3/16/20	sixthservice-developer[.]com

3/16/20	eithtservice-developer[.]com
3/17/20	servicedupdater[.]com
3/17/20	service-updateer[.]com
3/19/20	sexyservicee[.]com
3/19/20	serviceboostnumberone[.]com
3/19/20	servicedbooster[.]com
3/19/20	service-hunter[.]com
3/19/20	servicedhunter[.]com
3/19/20	servicedpower[.]com
3/19/20	sexycservice[.]com
3/23/20	yourserviceupdater[.]com
3/23/20	top-serviceupdater[.]com
3/23/20	top-servicebooster[.]com
3/23/20	serviceshelps[.]com
3/23/20	servicemonsterr[.]com
3/23/20	servicehunterr[.]com
3/23/20	service-helpes[.]com
3/23/20	servicecheckerr[.]com
3/23/20	newservicehelper[.]com
3/23/20	huntersservice[.]com
3/23/20	helpforyourservice[.]com
3/23/20	boostyourservice[.]com
3/26/20	developmasters[.]com

5/4/20	info-develop[.]com
5/4/20	ayechecker[.]com
5/4/20	service-booster[.]com
9/18/20	zapored[.]com
9/22/20	gtrsqer[.]com
9/22/20	chalengges[.]com
9/22/20	caonimas[.]com
9/22/20	hakunaman[.]com
9/22/20	getinformationss[.]com
9/22/20	nomadfunclub[.]com
9/22/20	harddagger[.]com
9/22/20	errvghu[.]com
9/22/20	reginds[.]com
9/22/20	gameleaderr[.]com
9/22/20	razorses[.]com
9/22/20	vnuret[.]com
9/22/20	regbed[.]com
9/22/20	bouths[.]com
9/23/20	ayiyas[.]com
9/23/20	serviceswork[.]net
9/23/20	moonshardd[.]com
9/23/20	hurrypotter[.]com
9/23/20	biliyilish[.]com

9/23/20	checkhunterr[.]com
9/23/20	daggerclip[.]com
9/23/20	check4list[.]com
9/24/20	chainnss[.]com
9/29/20	hungrrybaby[.]com
9/30/20	martahzz[.]com
10/1/20	jonsonsbabyy[.]com
10/1/20	wondergodst[.]com
10/1/20	zetrexx[.]com
10/1/20	tiancaii[.]com
10/1/20	cantliee[.]com
10/1/20	realgamess[.]com
10/1/20	maybebaybe[.]com
10/1/20	saynoforbubble[.]com
10/1/20	chekingking[.]com
10/1/20	rapirasa[.]com
10/1/20	raidbossa[.]com
10/1/20	mountasd[.]com
10/1/20	puckhunterrr[.]com
10/1/20	pudgeee[.]com
10/1/20	loockfinderrs[.]com
10/1/20	lindasak[.]com
10/1/20	bithunterr[.]com

10/1/20	sibalsakie[.]com
10/1/20	giveasees[.]com
10/1/20	shabihere[.]com
10/1/20	tarhungangster[.]com
10/1/20	imagodd[.]com
10/1/20	raaidboss[.]com
10/1/20	sunofgodd[.]com
10/1/20	rulemonster[.]com
10/1/20	loxliver[.]com
10/1/20	servicegungster[.]com
10/1/20	kungfupandasa[.]com
10/2/20	check1domains[.]com
10/5/20	sweetmonsterr[.]com
10/5/20	qascker[.]com
10/7/20	remotessa[.]com
10/7/20	cheapshhot[.]com
10/7/20	havemosts[.]com
10/7/20	unlockwsa[.]com
10/7/20	sobcase[.]com
10/7/20	zhameharden[.]com
10/7/20	mixunderax[.]com
10/7/20	bugsbunnyy[.]com
10/7/20	fastbloodhunter[.]com

10/7/20	servicewikii[.]com
10/7/20	secondlivve[.]com
10/7/20	quwasd[.]com
10/7/20	luckyhunterrs[.]com
10/7/20	wodemayaa[.]com
10/7/20	hybriqdjs[.]com
10/7/20	gunsdrag[.]com
10/7/20	gungameon[.]com
10/7/20	servicemount[.]com
10/7/20	servicesupdater[.]com
10/7/20	service-boosterr[.]com
10/7/20	serviceupdatter[.]com
10/7/20	dotmaingame[.]com
10/12/20	backup1service[.]com
10/13/20	bakcup-monster[.]com
10/13/20	bakcup-checker[.]com
10/13/20	backup-simple[.]com
10/13/20	backup-leader[.]com
10/13/20	backup-helper[.]com
10/13/20	service-checker[.]com
10/13/20	nasmastrservice[.]com
10/14/20	service-leader[.]com
10/14/20	nas-simple-helper[.]com

10/14/20	boost-servicess[.]com
10/14/20	elephantdrrive[.]com
10/15/20	service-hellper[.]com
10/16/20	top-backuphelper[.]com
10/16/20	best-nas[.]com
10/16/20	top-backupservice[.]com
10/16/20	bestservicehelper[.]com
10/16/20	backupnas1[.]com
10/16/20	backupmastter[.]com
10/16/20	best-backup[.]com
10/17/20	viewdrivers[.]com
10/19/20	topservicebooster[.]com
10/19/20	topservice-masters[.]com
10/19/20	topbackupintheworld[.]com
10/19/20	topbackup-helper[.]com
10/19/20	simple-backupbooster[.]com
10/19/20	top3-services[.]com
10/19/20	backup1services[.]com
10/21/20	backupmaster-service[.]com
10/21/20	backupmasterservice[.]com
10/21/20	service1updater[.]com
10/21/20	driverdwl[.]com
10/21/20	backup1master[.]com

10/21/20	checktodrivers[.]com
10/21/20	backup1helper[.]com
10/21/20	driver1updater[.]com
10/21/20	driver1master[.]com
10/23/20	view-backup[.]com
10/23/20	top3servicebooster[.]com
10/23/20	servicereader[.]com
10/23/20	servicehel[.]com
10/23/20	driver-boosters[.]com
10/23/20	service1update[.]com
10/23/20	service-hel[.]com
10/23/20	driver1downloads[.]com
10/23/20	service1view[.]com
10/23/20	backups1helper[.]com
10/25/20	idriveview[.]com
10/26/20	debug-service[.]com
10/26/20	idrivedwn[.]com
10/28/20	driverjumper[.]com
10/28/20	service1boost[.]com
10/28/20	idriveupdate[.]com
10/28/20	idrivehepler[.]com
10/28/20	idrivefinder[.]com
10/28/20	idrivecheck[.]com

First Seen	Server	Subject
12/12/19	140.82.60.155:443	CN=updatemanagir[.]us
12/21/19	96.30.192.141:443	CN=cmdupdatewin[.]com
1/6/20	45.76.49.78:443	CN=scrservallinst[.]info
1/8/20	149.248.58.11:443	CN=updatewinlsass[.]com
1/9/20	96.30.193.57:443	CN=winsystemupdate[.]com
1/14/20	95.179.219.169:443	CN=jomamba[.]best
1/16/20	140.82.27.146:443	CN=winsysteminfo[.]com
1/19/20	45.32.170.9:443	CN=livecheckpointsrs[.]com
1/20/20	207.148.8.61:443	CN=ciscocheckapi[.]com
1/28/20	209.222.108.106:443	CN=timesshifts[.]com
1/29/20	31.7.59.141:443	CN=updatewinsoftr[.]com
1/29/20	79.124.60.117:443	C=US
1/29/20	66.42.86.61:443	CN=lsassupdate[.]com
1/29/20	45.76.20.140:443	CN=cylenceprotect[.]com
1/29/20	45.76.20.140:80	CN=cylenceprotect[.]com
1/30/20	149.248.5.240:443	CN=sophosdefence[.]com
1/30/20	144.202.12.197:80	CN=windefenceinfo[.]com
1/30/20	149.248.5.240:80	CN=sophosdefence[.]com
1/30/20	149.28.246.25:80	CN=lsasswininfo[.]com
1/30/20	144.202.12.197:443	CN=windefenceinfo[.]com
1/30/20	149.28.246.25:443	CN=lsasswininfo[.]com

1/30/20	45.77.119.212:80	CN=taskshedulewin[.]com
1/30/20	149.28.122.130:443	CN=renovatesystem[.]com
1/30/20	45.32.170.9:80	CN=livecheckpointsrs[.]com
1/30/20	149.248.58.11:80	CN=updatewinlsass[.]com
1/30/20	149.28.122.130:80	CN=renovatesystem[.]com
1/30/20	207.148.8.61:80	CN=ciscocheckapi[.]com
1/31/20	81.17.25.210:443	CN=update-wind[.]com
1/31/20	31.7.59.141:80	CN=updatewinsoftr[.]com
2/2/20	155.138.214.247:80	CN=cleardefencewin[.]com
2/2/20	155.138.214.247:443	CN=cleardefencewin[.]com
2/2/20	45.76.231.195:443	CN=checkwinupdate[.]com
2/2/20	45.76.231.195:80	CN=checkwinupdate[.]com
2/3/20	46.19.142.154:443	CN=havesetup[.]net
2/3/20	95.179.219.169:80	CN=jomamba[.]best
2/3/20	140.82.60.155:80	CN=updatemanagir[.]us
2/3/20	209.222.108.106:80	CN=timesshifts[.]com
2/3/20	66.42.118.123:443	CN=conhostservice[.]com
2/4/20	80.240.18.106:443	CN=microsoftupdateswin[.]com
2/4/20	95.179.215.228:443	CN=iexploreservice[.]com
2/12/20	155.138.216.133:443	CN=defenswin[.]com
2/12/20	45.32.130.5:443	CN=avrenew[.]com
2/14/20	45.76.167.35:443	CN=freeallsafe[.]com
2/14/20	45.63.95.187:443	CN=easytus[.]com

2/17/20	95.179.147.215:443	CN=windefens[.]com
2/17/20	155.138.216.133:443	CN=defenswin[.]com
2/17/20	104.238.190.126:443	CN=aaatus[.]com
2/17/20	144.202.83.4:443	CN=greattus[.]com
2/17/20	104.156.245.0:443	CN=comssite[.]com
2/17/20	45.32.30.162:443	CN=bigtus[.]com
2/17/20	108.61.242.184:443	CN=livetus[.]com
2/17/20	207.148.15.31:443	CN=findtus[.]com
2/17/20	149.28.15.247:443	CN=firsttus[.]com
2/21/20	155.138.136.182:443	CN=worldtus[.]com
2/25/20	45.77.58.172:443	CN=freeoldsafe[.]com
2/25/20	45.77.58.172:443	CN=freeoldsafe[.]com
2/26/20	108.61.72.29:443	CN=myserviceconnect[.]net
2/27/20	216.155.157.249:443	CN=myserviceupdater[.]com
2/28/20	45.77.98.157:443	CN=topservicesbooster[.]com
2/28/20	104.156.250.132:443	CN=myservicebooster[.]com
2/28/20	149.28.50.31:443	CN=topsecurityservice[.]net
2/28/20	149.28.55.197:443	CN=myyserviceupdater[.]com
2/28/20	207.246.67.70:443	CN=servicesecurity[.]org
2/28/20	63.209.33.131:443	CN=serviceupdates[.]net
2/29/20	45.77.206.105:443	CN=myservicebooster[.]net
2/29/20	140.82.5.67:443	CN=servicesbooster[.]org
2/29/20	108.61.209.123:443	CN=brainschampions[.]com

2/29/20	140.82.10.222:443	CN=topservicesecurity[.]net
2/29/20	149.28.35.35:443	CN=topservicesecurity[.]org
2/29/20	207.148.21.17:443	CN=topserviceupdater[.]com
2/29/20	45.77.153.72:443	CN=topservicesupdate[.]com
3/1/20	140.82.10.222:80	CN=topservicesecurity[.]net
3/1/20	207.148.21.17:80	CN=topserviceupdater[.]com
3/1/20	108.61.90.90:443	CN=topservicesecurity[.]com
3/1/20	45.32.130.5:80	CN=avrenew[.]com
3/2/20	217.69.15.175:443	CN=serviceshelpers[.]com
3/2/20	155.138.135.182:443	CN=topservicesupdates[.]com
3/2/20	95.179.210.8:80	CN=serviceuphelper[.]com
3/2/20	45.76.45.162:443	CN=boostsecuritys[.]com
3/4/20	108.61.176.237:443	CN=yoursuperservice[.]com
3/4/20	207.246.67.70:443	CN=servicesecurity[.]org
3/6/20	188.166.52.176:443	CN=top-servicebooster[.]com
3/7/20	149.248.56.113:443	CN=topservicehelper[.]com
3/8/20	199.247.13.144:443	CN=hakunamatatata[.]com
3/8/20	95.179.210.8:443	CN=serviceuphelper[.]com
3/8/20	207.246.67.70:443	CN=servicesecurity[.]org
3/9/20	194.26.29.230:443	CN=secondserviceupdater[.]cor
3/9/20	194.26.29.229:443	CN=firstserviceupdater[.]com
3/9/20	194.26.29.232:443	CN=fourthserviceupdater[.]com
3/9/20	194.26.29.234:443	CN=sixthserviceupdater[.]com

3/9/20	194.26.29.236:443	CN=eighthserviceupdater[.]com
3/9/20	194.26.29.237:443	CN=ninethserviceupdater[.]com
3/9/20	194.26.29.225:443	CN=seventeenthservicehelper[.]
3/9/20	194.26.29.227:443	CN=nineteenthservicehelper[.]c
3/9/20	194.26.29.242:443	CN=thirdservicehelper[.]com
3/9/20	194.26.29.244:443	CN=tenthservicehelper[.]com
3/9/20	194.26.29.226:443	CN=eighteenthservicehelper[.]c
3/9/20	194.26.29.243:443	CN=ninthservicehelper[.]com
3/9/20	194.26.29.201:443	CN=secondservicehelper[.]com
3/9/20	194.26.29.202:443	CN=thirdservicehelper[.]com
3/9/20	194.26.29.220:443	CN=fourservicehelper[.]com
3/11/20	207.246.67.70:80	CN=servicesecurity[.]org
3/13/20	165.227.196.0:443	CN=twentiethservicehelper[.]cor
3/14/20	45.141.86.91:443	CN=thirdservice-developer[.]cor
3/14/20	194.26.29.219:443	CN=firstservisehelper[.]com
3/14/20	45.141.86.93:443	CN=fifthservice-developer[.]con
3/15/20	45.141.86.90:443	CN=secondservice-developer[.]
3/15/20	45.141.86.84:443	CN=firstservice-developer[.]con
3/17/20	45.141.86.96:443	CN=eithtservice-developer[.]cor
3/17/20	45.141.86.92:443	CN=fourthservice-developer[.]c
3/18/20	45.141.86.94:443	CN=sixthservice-developer[.]cor
3/18/20	108.61.209.121:443	CN=service-booster[.]com
3/18/20	134.122.116.114:443	CN=service-helpes[.]com

3/18/20	192.241.143.121:443	CN=serviceshelps[.]com
3/18/20	45.141.86.95:443	CN=seventhservice-developer[.]
3/18/20	198.211.116.199:443	CN=actionshunter[.]com
3/18/20	45.141.86.155:443	CN=sexyservicee[.]com
3/19/20	194.26.29.239:443	CN=eleventhserviceupdater[.]co
3/19/20	45.141.86.206:443	CN=servicedhunter[.]com
3/19/20	45.141.86.92:443	CN=service-updateer[.]com
3/19/20	134.122.116.59:443	CN=servicedbooster[.]com
3/19/20	134.122.118.46:443	CN=servicedpower[.]com
3/19/20	134.122.124.26:443	CN=serviceboostnumberone[.]c
3/20/20	45.141.86.97:443	CN=ninethservice-developer[.]c
3/20/20	178.62.247.205:443	CN=top-serviceupdater[.]com
3/20/20	159.203.36.61:443	CN=yourserviceupdater[.]com
3/20/20	134.122.20.117:443	CN=fifthserviceupdater[.]com
3/23/20	165.22.125.178:443	CN=servicemonsterr[.]com
3/24/20	69.55.60.140:443	CN=boostyourservice[.]com
3/24/20	45.141.86.98:443	CN=tenthservice-developer[.]co
3/26/20	178.79.132.82:443	CN=developmasters[.]com
3/26/20	194.26.29.247:443	CN=thirteenthservicehelper[.]co
5/4/20	159.65.216.127:443	CN=info-develop[.]com
9/22/20	69.61.38.155:443	C=US,ST=TX,L=Texas,O=lol,OU=
9/22/20	96.9.225.144:443	C=US,ST=TX,L=Texas,O=lol,OU=
9/22/20	96.9.209.216:443	C=US,ST=TX,L=Texas,O=lol,OU=

9/22/20	96.9.225.143:443	C=US,ST=TX,L=Texas,O=lol,OU=
9/22/20	69.61.38.156:443	C=US,ST=TX,L=Texas,O=lol,OU=
9/22/20	45.34.6.229:443	C=US,ST=TX,L=Texas,O=lol,OU=
9/22/20	45.34.6.226:443	C=US,ST=TX,L=Texas,O=lol,OU=
9/22/20	45.34.6.225:443	C=US,ST=TX,L=Texas,O=lol,OU=
9/22/20	107.173.58.185:443	C=US,ST=TX,L=Texas,O=lol,OU=
9/22/20	107.173.58.183:443	C=US,ST=TX,L=Texas,O=lol,OU=
9/22/20	107.173.58.175:443	C=US,ST=TX,L=Texas,O=lol,OU=
9/22/20	185.184.223.194:443	C=US,ST=CA,L=Texas,O=lol,OU=
9/22/20	109.70.236.134:443	C=US,ST=TX,L=Texas,O=lol,OU=
9/23/20	64.44.131.103:443	C=US,ST=TX,L=Texas,O=service
9/23/20	69.61.38.157:443	C=US,ST=TX,L=Texas,O=office,C
9/23/20	193.142.58.129:443	C=US,ST=TX,L=Texas,O=zapore
9/23/20	45.34.6.223:443	C=US,ST=TX,L=Texas,O=office,C
9/23/20	107.173.58.179:443	C=US,ST=TX,L=Texas,O=office,C
9/23/20	45.34.6.222:443	C=US,ST=TX,L=Texas,O=dagger,
9/23/20	107.173.58.180:443	C=US,ST=TX,L=Texas,O=office,C
9/23/20	107.173.58.182:443	C=US,ST=TX,L=Texas,O=office,C
9/23/20	45.34.6.221:443	C=US,ST=TX,L=Texas,O=office,C
9/24/20	213.252.244.62:443	C=US,ST=TX,L=Texas,O=lol,OU=
9/24/20	185.25.50.167:443	C=US,ST=TX,L=Texas,O=office,C
9/30/20	88.119.171.75:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.171.74:443	C=US,ST=TX,L=Texas,O=lol,OU=

10/1/20	88.119.171.67:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.171.76:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.171.68:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.171.69:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.171.73:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.171.77:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.171.78:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	213.252.244.38:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	107.173.58.184:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.174.109:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.174.110:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.174.114:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.174.116:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.174.117:443	C=US,ST=TX,L=TExas,O=lol,OU=
10/1/20	88.119.174.118:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.174.119:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.174.121:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.174.120:443	C=US,ST=TX,L=Texas,O=office,C
10/1/20	88.119.174.107:443	C=US,ST=TX,L=Texas,O=office,C
10/1/20	88.119.174.125:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.174.126:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.174.127:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	88.119.174.128:443	C=US,ST=TX,L=Texas,O=lol,OU=

10/1/20	213.252.244.170:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/1/20	213.252.246.154:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/5/20	5.2.64.113:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	5.2.79.122:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	88.119.171.94:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	5.2.64.133:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	5.2.64.135:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	5.2.72.202:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	88.119.175.153:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	213.252.245.71:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	213.252.246.144:443	C=US,ST=TX,L=Texas,O=US,OU=
10/7/20	5.2.64.149:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	5.2.64.144:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	88.119.174.139:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	88.119.174.133:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	88.119.175.214:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	5.2.72.200:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	5.2.79.10:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	5.2.79.12:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	5.2.79.121:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	5.2.64.174:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	5.2.64.172:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	5.2.64.167:443	C=US,ST=TX,L=Texas,O=lol,OU=

10/7/20	88.119.171.97:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	88.119.171.96:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	96.9.209.217:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/7/20	69.61.38.132:443	C=US,ST=CA,L=Mountainvew,O=
10/13/20	45.147.230.131:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/13/20	45.147.229.92:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/13/20	45.147.229.68:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/13/20	45.147.229.52:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/13/20	45.147.229.44:443	C=US,ST=TX,L=Texsa,O=lol,OU=
10/14/20	45.147.230.87:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/14/20	45.147.230.159:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/14/20	45.147.230.141:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/14/20	45.147.230.140:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/14/20	45.147.230.133:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/14/20	45.147.230.132:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/14/20	45.147.229.180:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/14/20	45.147.230.159:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/15/20	45.147.230.132:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/15/20	45.138.172.95:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/16/20	108.62.12.119:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/16/20	108.62.12.105:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/16/20	108.62.12.114:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/16/20	108.62.12.116:443	C=US,ST=TX,L=Texas,O=lol,OU=

10/16/20	45.147.230.140:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/16/20	45.147.230.133:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/19/20	74.118.138.137:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/19/20	74.118.138.115:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/19/20	108.177.235.53:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/19/20	74.118.138.138:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/21/20	45.153.241.1:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/21/20	45.153.240.240:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/21/20	45.153.240.194:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/21/20	45.153.240.138:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/21/20	45.153.240.136:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/23/20	45.153.240.157:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/23/20	45.153.240.178:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/23/20	45.153.240.220:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/23/20	45.153.240.222:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/23/20	45.153.241.134:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/23/20	45.153.241.138:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/23/20	45.153.241.146:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/23/20	45.153.241.153:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/23/20	45.153.241.158:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/23/20	45.153.241.167:443	C=US,ST=TX,L=Texas,O=US,OU=
10/23/20	45.147.231.222:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/23/20	45.153.241.141:443	C=US,ST=TX,L=Texas,O=lol,OU=

10/26/20	108.62.12.12:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/26/20	108.62.12.121:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/26/20	172.241.27.65:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/26/20	172.241.27.68:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/26/20	172.241.27.70:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/26/20	45.153.241.139:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/27/20	45.153.241.14:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/28/20	190.211.254.154:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/28/20	81.17.28.70:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/28/20	81.17.28.105:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/28/20	179.43.160.205:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/28/20	179.43.158.171:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/28/20	179.43.133.44:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/28/20	179.43.128.5:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/28/20	179.43.128.3:443	C=US,ST=TX,L=Texas,O=lol,OU=
10/28/20	81.17.28.122:443	C=US,ST=TX,L=Texas,O=lol,OU=

RYUK CommandsRYUK Commands

```
start wmic /node:@C:\share$\comps1.txt /user:[REDACTED] /pa
start PsExec.exe /accepteula @C:\share$\comps1.txt -u [REDA
start PsExec.exe -d @C:\share$\comps1.txt -u [REDACTED] -p
```

Detecting the Techniques

FireEye detects this activity across our platforms. The following table contains several specific detection names from a larger list of detections that were available prior to this activity occurring.

Endpoint Security	• KEGTAP INTERACTIVE CMD.EXE CHILD PROCESS (BACKDOOR) • KEGTAP DLL EXECUTION VIA RUNDLL32.EXE (BACKDOOR) • SINGLEMALT (DOWNLOADER) • STILLBOT (BACKDOOR) • WINEKEY (DOWNLOADER) • CORKBOT (BACKDOOR) • RYUK RANSOMWARE ENCRYPT COMMAND (FAMILY) • RYUK RANSOMWARE SETUP EXECUTION (FAMILY) • RYUK RANSOMWARE WAKE-ON-LAN EXECUTION (FAMILY) • RYUK RANSOMWARE STAGED ENCRYPTOR INTERNAL TRANSFER TARGET (UTILITY) • RYUK RANSOMWARE ENCRYPTOR DISTRIBUTION SCRIPT CREATION (UTILITY) • RYUK RANSOMWARE STAGED ENCRYPTOR INTERNAL TRANSFER SOURCE (UTILITY)
Network Security and Email Security	• Downloader.Win.KEGTAP • Trojan.KEGTAP • APTFIN.Backdoor.Win.BEERBOT • APTFIN.Downloader.Win.SINGLEMALT • APTFIN.Backdoor.Win.STILLBOT • APTFIN.Downloader.Win.WINEKEY • APTFIN.Backdoor.Win.CORKBOT • FE_Downloader_Win64_KEGTAP • FE_APTFIN_Backdoor_Win32_BEERBOT • FE_APTFIN_Backdoor_Win_BEERBOT • FE_APTFIN_Downloader_Win32_SINGLEMALT • FE_APTFIN_Downloader_Win64_SINGLEMALT • FE_APTFIN_Backdoor_Win_STILLBOT • FE_APTFIN_Downloader_Win_WINEKEY • FE_APTFIN_Backdoor_Win_CORKBOT

Posted in Threat Intelligence—Security & Identity

Threat Intelligence

Hybrid Russian Espionage and Influence Campaign Aims to Compromise Ukrainian Military Recruits and Deliver Anti-Mobilization Narratives

By Google Threat Intelligence Group • 10-minute read

Threat Intelligence

Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575)

By Mandiant • 19-minute read

Threat Intelligence

How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends

By Mandiant • 10-minute read

Threat Intelligence

capa Explorer Web: A Web-Based Tool for Program Capability Analysis

By Mandiant • 6-minute read