TLP:WHITE

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Investigation ‘Bonfire’

From a single LockerGoga infection to analysing a large part of the infrastructure used by at least two adversaries

Intended for general release by NCSC-NL

1 Summary

More and more ransomware attacks are being observed worldwide, which are specifically targeted towards large companies. In some campaigns the goals of the actors is to collect a large sum of ransom payments. These ransom payments vary between tens of thousands to millions of euro's per victim.

In March 2019, NCSC-NL started an investigation into a specifically targeted ransomware campaign, named LockerGoga. The reason for this investigation was a report at NCSC-NL of a ransomware infection at a Dutch office of an international supplier in the chemicals sector, which has a key role in supporting critical infrastructure.

The NCSC-NL investigation was aimed at finding (future) ransomware attacks towards the Dutch central governmental or critical infrastructure. In addition, the goal of this investigation was to determine a modus operandi of the actor(s) involved to recognize and prevent (further) attacks as well notifying victims that were compromised, but did not face a ransomware deployment (the final stage) yet. Information could be used to mitigate or prevent any further damage. During this investigation, NCSC-NL learned that part of the infrastructure was hosted within the Netherlands.

In NCSC-NL's investigation, over 1.800 unique IP addresses from organisations worldwide have been identified as a victim that has been compromised, as a possible target for ransomware or other attacks. Among the victims, there are multiple Dutch organisations and foreign multinationals with Dutch branches. The actual number of victims is probably considerably higher, because NCSC-NL currently only has insight into a small part of the infrastructure that is being used by the attackers.

Organisations within the central government and critical infrastructure in the Netherlands are currently not identified as a victim of the campaign. In other countries these kind of organisations already became a victim and in the Netherlands supply chain partners and suppliers of the central government and critical infrastructure have been hit.

NCSC-NL informed victims using its international CSIRT and CERT networks. Even when a victim was informed about a compromise, it has proven very difficult to locate and fully remediate the compromise. In several cases a victim has previous hints of a compromise, but was unable to locate it, even though these companies had a very knowledgeable IT and/or (external) incident response team. After a victim received technical information such as compromised accounts, computers, C2 IP ranges, etc. from our investigation, they were able to identify the breach. With this specific information, many companies were able to prevent ransomware from being deployed as well as preventing the attacker to gain access to the network again.

Based on the C2 servers, their history and OSINT we suspect these servers have been deployed as early as July 2018. Activity has however only been observed since October 2018. On 26 October 2021 Europol [1] together with several law enforcement agents have targeted 12 individuals in a police operation. As the result of the action day, over USD 52 000 in cash was seized, alongside 5 luxury vehicles. A number of electronic devices are currently being forensically examined to secure evidence and identify new investigative leads.
[1] https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure

Index

Index

2 Threat Analysis

2.1 Actors

While attribution is not the primary focus of our investigation or for NCSC-NL in general, it helps us in getting a better assessment of the modus operandi of the attackers.

There are indications that multiple actors are using the infrastructure that is used in the LockerGoga campaign. At this time, there is limited insight into the criminal network and modus operandi. These actors are cybercriminal groups pursuing financial gain. Whether there are possible links to state actors is unknown.

2.2 Motive

It is likely that attackers spread the LockerGoga-ransomware for financial gain. After encryption, victims are asked to contact the attackers by e-mail or approached by phone to pay ransom. There are cases in which the systems were successfully decrypted after payment. Other motives, such as espionage and sabotage, can however not be excluded. At several victims, there are indications that large amounts of data were exfiltrated and industrial control systems were manipulated

2.3 Modus operandi

Based on the information that is currently available, a likely hypothesis is:

One actor performs the first part of the attacks in order to gain access to the company networks of the victims. This actor sells the access to the company network to a second actor (directly or via the dark web), who performs the second part of the attack (exfiltrate data, spread ransomware and/or manipulate systems). The second actor can be pursuing financial gain, but espionage and sabotage can be a motive as well.

The attackers probably use different methods to gain access to the company networks. Next, they will explore the network. Later (often after several months), the LockerGoga ransomware is spread. The modus operandi in the LockerGoga campaign, a targeted ransomware attack, is not new. Earlier examples are the Ryuk, GandCrab and Samas ransomware campaigns.

The actors responsible for the attacks seem to be highly qualified. The attackers infiltrated the networks of hundreds, maybe even thousands, of organisations worldwide. Among the victims are several organisations with a lot of experience in cybersecurity as well. Furthermore, the attackers are able to retain access to the targeted network for months and avoid detection when moving laterally through the network.

2.4 Mitigation strategies

There are indications that unique LockerGoga variants are generated for each victim. Indicators that were collected during the investigations of previous attacks, such as file hashes, therefore have very limited value for detection. NCSC-NL has been able to share more generic detection indicators with its partners that can be used to detect the LockerGoga attackers on the internal network.

There are known cases where contact with the attackers took place after payment and decryption was successful. As far as we know, the decryption key only decrypts files that are encrypted with a specific version and public key that was deployed at one specific victim and therefore cannot be used for other victims.

2.4.1 Preventing further damage

NCSC-NL has identified many victims based on extensive research. A victim is an organisation where attackers have compromised the network. These are organisations from which network communication with the C2 servers used by the attackers has been observed. The ransomware has not (yet) been deployed for all of these victims. During this investigation, most of the concerning organisations that we encountered were informed with help from our international CERT-network so that they could take measures to prevent further infection and deployment of ransomware. This has prevented a lot of damage.

2.5 Victim overview

2.5.1 Number of victims

To date, more than 1.800 unique IP addresses of organisations worldwide have been identified as victims in the investigation. The actual number of victims will most likely be considerably higher, because NCSC-NL currently only has a limited view of the infrastructure used by the attackers.

2.5.2 Affected sectors and geographical distribution

An analysis of the list of victims identified by the NCSC shows that a lot of the organisations affected are multinational companies and have branches in several countries. The affected organisations fall into various sectors, including automotive, construction, chemical, consultancy, metal, entertainment, IT, government, production, retail and healthcare. In general, these are large companies with a turnover of several millions or billions of euros.

Both a very limited amount of Dutch organisations and foreign multinationals with Dutch branches are among the victims. At this time, no infections have been observed within the Dutch central government and critical infrastructure providers. The victims do include chain partners and suppliers of Dutch central government and critical infrastructure providers.

2.6 Impact

The activities of cyber criminals have a major potential impact on national security. Society and economy have become completely dependent on digital resources. The consequences of attacks and outages can be large and even disruptive to society.

The financial impact of the LockerGoga campaign is its most visible aspect. The damage caused for an affected organisation easily runs into tens of millions of euros to remediate the attack, not including the ransomware demand. For example the Norwegian energy and aluminum group Hydro is currently estimating more than 40 million euros in damages. Other known ransomware infections also led to millions of damage.

The LockerGoga campaign seems to be aimed at large organisations, such as multinationals and production companies. Ransomware attacks on this type of organisation have both direct and indirect (financial) consequences:

- Several organisations will decide to pay large amounts of ransom to decrypt their systems.
- Incident response, (forensic) investigation and recovery must be carried out, before systems can be restored.
- Because of the risk of persistent access, organisations are forced to replace their systems, even when they have paid for decryption.
- The production process can come to a halt for a longer period of time, sometimes weeks. Potentially resulting in large economic damages and resulting chain effects on other dependent companies.
- Employees cannot work for a longer period of time, sometimes for weeks. For example, they cannot connect to the corporate network and have no access to their e-mail.
- Media attention causes reputational damage, which can lead to loss of customers or affect stock price(s).

The attacks are highly profitable for the attackers. For some organisations, the significant impact of a ransomware infection has been the reason to pay hundreds of thousands or sometimes even millions of euros in ransom, also in The Netherlands. It is therefore not to be expected that the attackers will quit the attacks by themselves as it is very profitable. Because the chance is high that the attackers have persistent access to the company network, a large part of, if not all, systems have to be replaced, even when ransom has been paid.

Because it is plausible that there are actors involved with other motives than financial gain, such as espionage or sabotage, the threat is broader than the risk of being infected with ransomware. Access to companies might be sold on black markets. As a result of a compromise (sensitive) information can be exfiltrated and used for other purposes. Cyber-attacks on organisations in the production and (petro)chemical industry for example, can form a threat to safety, health and environment as well.

https://www.reuters.com/article/us-norway-cyber/norsk-hydros-initial-loss-from-cyber-attack-may-exceed-40-million-idUSKCN1R71X9

3 Tactics, Techniques and Procedures (TTPs)

Based on extensive research and collaboration with other entities we were able to identify some of the C2 servers. These collections are based on this research as well as information received from victims.

3.1 Getting a foothold within the target network

3.1.1 Initial breach

We do not have much information of the initial beaches, however based on reports from victims and some beacon logs we can see a period of time (usually several months) passing between the initial breach and exploitation of the victim's infrastructure. The method used to initially breach the network perimeter varies but is reported to be:

- Bruteforce attacks against publicly reachable RDP servers
- Attacks on vulnerable external services, e.g. a public website vulnerable for SQL Injections.
- Dropping malware on a target system, e.g. by adding a payload into a Word document
- Phishing (by using data from a not yet reported data breach at a large online retailer)
- Compromised personal system(s) of an employee, which contain cached credentials for work systems
- Compromised work system(s) of an employee, where credentials are collected from the system using a InfoStealer
- Usage of 0-day exploits to gain access to a system
- Usage of 0-day exploits to gain privileged access on the system

After the breach and exploitation to privileged network access there is not much activity found on any of the compromised systems. We assume this is a period where the actor will try to sell their gained access to another actor.

3.1.2 Sold access to another actor

After the period of no activity, activity spikes up again. This time most of the activity is done and logged through the C2 servers. Based on these logs we were able to reconstruct a large part of the process. This process repeats, sometimes with slight variations, which can be outlined as:

- Discovery through dumping Active Directory
- Discovery though scanning
- Lateral movement though WMIC and Powershell
- Collecting administrative event logs
- Usage of known and unknown vulnerabilities
- Creating persistence
- Disabling or corrupting backups
- Data exfiltration and waiting period
- Deployment of ransomware
- Communication between victim and attackers
- Re-establishing contact with compromised servers

3.2 Discovery through dumping Active Directory

Once a beacon has connected to the C2 server, one of the first actions the attacker takes is to create an inventory of the Active Directory. Based on the data we received, the attackers used Adfind for each victim and the commands passed to each victim never changed while observing the attacker. In several cases, ntdsutil was used to create a binary backup of the Active Directory. These files can be exfiltrated to the C2 server using several Cobalt Strike features or by using other tools such as DNScat2. As most companies cannot be identified with their IP address alone, these dumps, still located on the C2 servers, contain company and employee information, which allowed us to identify some of the companies that have been compromised.

3.2.1 Observed commands

- net view
- net view /DOMAIN
- nltest /dclist
- adfind.exe -f (objectcategory=person) > ad_users.txt
- adfind.exe -f objectcategory=computer > ad_computers.txt
- adfind.exe -f (objectcategory=organisationalUnit) > ad_ous.txt
- adfind.exe -subnets -f (objectCategory=subnet) > ad_subnets.txt
- adfind.exe -f "(objectcategory=group)" > ad_group.txt
- adfind.exe -gcb -sc trustdmp > ad_trustdmp.txt
- 7.exe a dcc.7z *.txt
- 7.exe a -mx3 dc.7z *.txt
- Powershell (Get-ADComputer)
- "ntdsutil \"activate instance ntds\" \"ifm\" \"create full C:\windows\temp\ntds\" quit quit"

3.3 Collecting data from compromised system

While analyzing the artifacts found on the C2 servers, we not only found that the attackers were collecting Active Directory dumps but also screenshots, files/documents and even audio recordings. We do not know for what purpose these are collected, but we have reason to assume they might do this to identify the company they gained access to or another actor setting out actions other than with a financial motive.

3.4 Discovery through scanning

3.4.1 Nslookup

The attackers use nslookup to find the IP addresses for each system discovered in Active Directory dumps by importing the hosts into Cobalt Strike and/or Armitage. Using default functionality, it sends single or bulk commands to the beacon to get the IP address for each of the discovered system.

3.4.1.1 Observed commands

- Host: nslookup HOSTNAME
- Bulk: nslookup HOSTNAME >> ns2.txt & nslookup HOSTNAME >> ns2.txt & ....
  Note: the output filename may differ, mostly adding or changing a number

3.4.2 Ping

Once all the target hosts have been resolved to IP addresses, a ping-sweep is done to all these hosts to target online systems only. Using default functionality, Armitage or Cobalt Strike sends single or bulk commands to the beacon to get the online status for each of the discovered system's IP address. In some cases, the attacker pings entire subnets found in the Active Directory.

3.4.2.1 Observed commands

- Host: ping HOSTNAME
- Bulk: ping HOSTNAME >> ping.txt & ping HOSTNAME >> ping.txt & ....
  Note: the output filename may differ, mostly adding or changing a number. In some instances a "–n 1" flag was added

3.4.3 Mass scanning

Mass scanning on ports 135, 445, 338[0-9] but only on IP addresses or IP subnets discovered in Active Directory

3.4.3.1 Observed commands

- masscan.exe REDACTED -p135 --rate=1000 -oG mass_log.txt
- masscan.exe REDACTED -p445 -oG myhost445.txt
- masscan.exe -iL ips_all.txt -p3389 --rate=305 -oG 3389log.txt
- masscan.exe -iL ips_all.txt -p445 --rate=305 -oG 445log.txt
- portscan REDACTED 445
- portscan REDACTED 3381
- portscan REDACTED 3389

3.5 Lateral movement through WMIC and Powershell

Call to wmic, powershell, etc. for discovery to get target systems information.

3.5.1 Disabling AntiVirus/Endpoint protection

Instances have been observed where AV software from Kaspersky was copied to a victim's machine. The reasons for doing so is not clear, yet the assumption is that this is likely used to remove existing endpoint protection software, as most AV installers have an option to trigger an uninstallation of existing products to prevent conflicts. We have no indications that software from Kaspersky is used beyond the triggering of the installation process, no modifications were observed and the installation itself was likely cancelled after the old AV product was removed. Starting an uninstallation process for existing endpoint protection software manually is more likely to be blocked or might require user intervention.

3.5.2 Getting system information

For each of the compromised systems the attacker tries to profile the system by querying as much details as possible.

3.5.2.1 Observed commands

- wmic /node:"REDACTED" os get caption
- wmic /node:"REDACTED" /"user:"REDACTED /"password:"REDACTED" process list
- wmic /node:"REDACTED" /"user:"REDACTED /"password:"REDACTED" process list brief
- powershell Get-ADComputer
- C:\Windows\System32\netstat -anop tcp
- C:\Windows\System32\net use
- C:\Windows\System32\query.exe session
- C:\windows\system32\systeminfo.exe
- c:\Windows\System32\ipconfig.exe /all

3.5.3 Finding administrators

To expand on the initial footprint, the attackers collect more information about the administrators in the domain and their information. Getting administrative access to the domain simplifies further actions by the attackers.

3.5.3.1 Observed commands

- powershell -C "import-module .\admins.ps1"
- powershell -C "import-module .\hashdump.ps1"
- powershell -C "[intptr]::size"
- powershell -ep bypass -C "dsquery * -filter (samaccoutname='domain admin') | dsget group -members -expand"
- powershell -ep bypass -C "import-module .\admins.ps1"
- C:\Windows\system32\net group "domain admins" /domain

3.5.4 Collecting Credentials and hashes

The C2 servers kept logs from the attacker, including a record of all credentials captured by the attackers. These vary from hashes extracted from systems to collected plain-text credentials. On one of the administrative systems several files where found that contained known hash and password combinations, which simplifies the collecting of clear-text passwords. On average over hundreds of accounts where collected from each network and stored. This allows the attacker to reuse these accounts for future compromises of the same network.

3.5.4.1 Observed commands

- mimi "lsadump::dcsync /domain:REDACTED /user:REDACTED" exit > REDACTED

3.6 Collecting administrative event logs

We think the actors uses the Windows security logs to find systems from which system administrators are logging in. They are likely specifically targeting these systems as these systems are used by privileged users and could be used for additional lateral movement, for example if the attackers gained access to a subset of the Active Directory they might find credentials to access to parent Active Directory domains.

3.6.1 Observed commands

- get-eventlog 'Security' | where {$_.Message -like '*admin*' -AND 'Source Network Address'} | export-csv c:\temp\events_admin.txt
- get-eventlog 'Security' | where {$_.Message -like '*Totality*' -AND 'Source Network Address'} | export-csv c:\temp\events_admin.txt

3.7 Usage of vulnerabilities

3.7.1 Known vulnerabilities

Armitage session logs show a partial history of Metasploit vulnerabilities used within the campaign. The logs contain a list of systems within victim organisations, where for each system a list of exploitable vulnerabilities were successfully used by the actor.

The logs show that the exploited vulnerabilities are known Microsoft Windows vulnerabilities listed in the Microsoft Security bulletin 17-010 (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147 and CVE-2017-0148). These vulnerabilities are all related to how the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests, and all the compromised systems seen still have SMBv1 enabled.

In some instances CVE-1999-0504 was used, which shows that systems have a local administrator account with a default, null, blank or missing a password.

3.7.2 Unknown vulnerabilities (oday)

Session logs from the C2 servers also show uploading of files and executing of specific exploits. Based on the commands given and the upload folders (containing "oday" in its name) there are hints that 6 or 7 oday's are in the possession of the actor.

One of the victims reported they have located one of these oday's on their compromised systems, which is a Microsoft Windows privilege escalation exploit. They have reported this to Microsoft and they learned that Kaspersky also reported [1] this oday and was fixed in the Patch Tuesday of April 9th. The initial breach at the victim using this exploit was found in logs early October 2018. This means this oday was actively used between October 2018 (likely even since July 2018) and April 2019 based on the logs from this victim.

On the administrative Windows system we found tools like RDP brute and RDP recognizer, including logs that show these tools have been used. The resulting data sets were found on the desktop and split between NLA enabled and non-NLA enabled RDP servers. The data set is likely split out due to the requirement of a different attack vector for each of these categories.

[1] https://www.kaspersky.com/blog/cve-2019-0859-detected/26451/

3.7.3 Usage of Layer 2 VPN tunnels

The attacker uses VPN software such as AnyDesk and Hamachi to create a layer 2 tunnel to the victim's network. This allows the attacker to use his preferred 'workstation' for attacks. This is probably used to protect the special and/or unknown exploits and vulnerabilities to attack the victim's network. Based on the logs from the C2 servers the attacker remotely mounts a share from the attackers system and the name used from the local file system mount suggest it has been mounted using a VeraCrypt container. This is most likely done so that the attacker does not need to create copies of exploits on C2 or other intermediary servers.

3.8 Creating persistence

3.8.1 Enabling RDP Access

The attacker makes firewall and registry changes to enable or disable RDP on the private (trusted) profile of the victim system. The attacker mainly uses the default port (3389) but the attacker has also been using ports within the range 3380-3390.

3.8.1.1 Observed commands

- Netsh.exe advfirewall firewall add rule name="mstsc" program="c:\windows\system32\mstsc.exe" protocol=tcp dir=in enable=yes action=allow profile=Private
- Reg add "\\5249\HKLM\SYSTEM\CurentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d /f
- reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
- reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber" /v 3389
- reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber" /v fDenyTSConnections /t REG_DWORD /d 0 /f
- reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber" /v fDenyTSConnections /t REG_DWORD /d 3380 /f
- reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber" /v fDenyTSConnections /t REG_DWORD /d 3389 /f

3.8.2 Creating Active Directory, Local and SQL users

Creation of new Windows Active Directory, Local and Microsoft SQL users. These are then added to the 'Administrators', 'Domain Admins', 'Remote Desktop Users', 'Enterprise Admins' and other privileged groups and used for lateral movement and collecting more credentials. Throughout the campaign, the attacker has been seen using the same usernames and a few variations on them.

3.8.2.1 Observed commands

- powershell Add-AdGroupMember -Identity "Domain Admins" –Members terminal
- net group "domain admins" admin_svc /domain /add
- net group "domain admins" /domain terminal /add
- net localgroup "Administrators" svc /add
- net localgroup administrators terminal /add
- net user admin_svc Qwe_321@ /add /domain
- net user rapid_svc Qwe_321@ /add /domain
- osql -E -S -Q "CREATE LOGIN [admusr] WITH PASSWORD=N'qwe123', DEFAULT_DATABASE=[master], CHECK_EXPIRATION=OFF, CHECK_POLICY=OFF;EXEC master..sp_addsrvrolemember @loginame = N'admusr', @rolename = N'sysadmin'"
- osql -E -S -Q "select * from master.sys.server_principals"
- osql -E -S -Q "select @@version"

3.8.2.2 Observed created Windows users and passwords:

admin_svc	Qwe_321@		
terminal	O3Ded!@#	O3DeD!@#	P2SwS!@#
rapid_svc	Qwe_321@		
svc23	Qwe_321@		
svc1	Qwe_321@		
svc	Qwe_321@	QweQwe_321@	
vdp	Qwe_321@		
s-backup	O3DeD!@#		

3.8.2.3 Observed created Microsoft SQL users and passwords:

admuser	qwe123

3.9 Disabling or corrupting backups

Although we did not yet observe these actions ourselves, we do have reports from victims that the actor tried to disable (e.g. through encryption) or corrupt the backups, in some cases successfully. This is likely to prevent the victim from restoring their infrastructure from backups and to create an additional incentive to pay the ransom.

3.10 Waiting period

A very interesting fact is the amount of time the attacker(s) are in the victim's network, where the attacker has gone unnoticed for even more than 7 months. There seems to be two distinctive periods where no activity has been observed and the beacons are idle:

- Between the initial infection and post exploitation. This is likely the time the actor that initially breached the network needs to sell the credentials, either to trusted partners or through underground marketplaces.
- Between post exploitation and the deployment of ransomware. This is likely the time in which the attacker will try to corrupt or encrypt the backups and wait in attempt to make sure all known good backups have rotated out, or the attacker needed to create a victim profile. In addition, preparations need to be made on the attacker side, such as creating two e-mail addresses, buying the malware, etc.

3.11 Data exfiltration

We have observed the attacker exfiltrating data such as Active Directory information from all users and locations. In some cases the attacker also downloaded all webcontent (entire webroot folder) as well as full database dumps. From victims we are in contact with we know that they also downloaded sensitive corporate information like software and data. For example, the CityComp [1] hack can be directly linked to the same C2 infrastructure and the compromise of an AV vendor, where debug symbols were obtained, which the attacker thought to be source code.

[1] https://www.vice.com/en_us/article/d3np4y/hackers-steal-ransom-citycomp-airbus-volkswagen-oracle-valuable-companies

3.12 Deployment of ransomware

Although the moment the attacker deploys ransomware within the target network is unknown, we believe that several conditions are a factor, such as making sure the backup retention has been rotated out.

The attackers do not use the newly created (privileged) accounts, but rather used compromised privileged accounts. We assume this is done to prevent the discovery of these newly created accounts and keep persistent access on the network after deployment of the ransomware.

3.12.1 Code signing

Digital certificates cryptographically vouch for the trustworthiness of the software's publisher. They tell an operating system that the software is legitimate. Therefore, malware creators have long tried to use certificates to increase the chances of their creations to go undetected by anti-malware measures. A recent study has found that malware is increasingly signed by legitimate certificates, obtained directly or indirectly from certificate authorities (CA) or their resellers. This is in contrast with an earlier trend that if malware was signed, it was usually done with a stolen certificate. Most of the digital certificates used to sign malware samples found on VirusTotal in 2018 have been issued by the Certificate Authority (CA) Comodo CA (aka Sectigo).

Source: "Malware authors increasingly use legitimate certificates to bypass defences", by CERT-EU reference: 190524-1 published 24 may 2019 and https://medium.com/@chroniclesec/abusing-code-signing-for-profit-ef80a37b50f4

3.12.2 Ransomware families

The C2 server logs show the usage of both LockerGoga and MegaCortex families on victim systems. The ransomware is transported to the compromised system by creating a binary pastebin.com download. From other reports we have collected rerference to Ryuk and RietSpoof are made as well, however could not be observed by our investigation so far. A more detailed report on these families can be found in chapter 5

3.12.2.1 Observed commands

- psexec.exe \\REDACTED -u "REDACTED" -p "REDACTED" -d -h –r mstscupd -s -accepteula -nobanner c:\windows\temp\win64_update.exe REDACTED (<- contain MegaCortex base64 hash required to start)
- psexec.exe \\REDACTED -u "REDACTED" -p "REDACTED" -d -h –r mstscupd -s -accepteula -nobanner c:\windows\temp\win32.bat
- powershell Restart-Computer -ComputerName REDACTED –Force
- powershell Restart-Computer -ComputerName "REDACTED" –Protocol WSMan -WSManAuthentication Kerberos

3.13 Re-establishing contact with compromised servers

The attackers will actively keep trying to attack (cleaned) victim systems, even after the victim has made payment, traffic has been seen from the attackers' infrastructure towards the victim's network. In another case, C2 beacons were observed from the infrastructure to a victim that paid the ransom months before and 'assumed' their network to be clean.

In some cases, the victim did not pay the ransom and removed the infection. One known case, where a victim replaced their infra, the attackers managed to regain access to the network. It is unknown how they regained access, but it is very likely they previously collected username and passwords that were reused after the reinstallation of the network.

3.14 Specific targetting

We see Cobalt Strike beaconing from IP addresses that either come from TOR exit-nodes or known security research networks. We assume that these connections are initiated by researchers in an attempt to get the attacker to send commands to their research environment. However looking at the C2 logs the attacker ignores them or sends and 'exit' command to that beacon. The attackers seems to have a good overview of targets and systems that do not belong within the C2 network.

4 Ransomware families used

4.1 Observed families

During this investigation, Ryuk, LockerGoga and MegaCortex ransomware were deployed at victim organisations. Although none of the ransomware samples were found on the servers analyzed, correlation between attacker activity seen in the logs and reporting of incidents at victims clearly shows these malware families being used.

4.1.1 Ryuk

Out of the three mentioned ransomware families, Ryuk was the first to be seen in the wild. The first occurences of Ryuk were seen around August 2018. Ryuk seems to be a modified version of HERMES ransomware, sharing similarities in code and behavior such as whitelisted folders and dropped files.

When the Ryuk ransomware is started, it first attempts to kill or stop a number of predefined processes and services. These processes and services are related to software that could prevent or remediate the encryption process, such as antivirus or backup software. The Ryuk ransomware now makes itself persistent on reboots through a registry key, making sure it is run every time the victim system boots.

The encryption process used by Ryuk relies on both symmetrical (AES) as well as asymmetrical (RSA) cryptography. The attackers use a robust and effective way to encrypt the files, by creating unique public/private RSA key pairs per victim, and by creating a new AES key for each file to be encrypted. Without the required RSA private key, which is only in possession of the attacker, decryption is impossible. Unique RSA key pairs per victim mean that a decryption tool or private RSA key for one victim, cannot be reused at other victims.

Ryuk encrypts all files, except for files with the .exe, .dll, .ini, .lnk or .hrmlog extensions. Ryuk has a list of whitelisted directories where encryption should not take place, to make sure the basic operating system and applications such as browsers still work. Besides encryption on the local system, Ryuk also attempts to encrypt files on all network drives it can find and has write access to. All encrypted files will have the .ryk extension appended to them. It will then drop ransom notes on the victim system, containing email addresses to contact the attackers. In older versions, this ransom note also included a BTC wallet address, which is no longer present in recent versions.

https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/

4.1.2 LockerGoga

LockerGoga is a new ransomware family that was first seen in the January 2019. It has several noteworthy differences compared to Ryuk in how it is deployed by attackers and how the malware operates.

Where Ryuk can encrypt data on network shares as well, LockerGoga only encrypts data on the system it runs on. This means that attackers need to have access to all systems they want to encrypt data on. As described in this report, the attackers are seen actively obtaining information on relevant systems within victim organisations, as well as obtaining login information through, for example, Active Directory dumps. With this information, attackers are able to remotely deploy LockerGoga through psexec on each of the systems they deem relevant to encrypt.

When LockerGoga is executed on a target system, the malware does not use any method to ensure persistence on reboot. It copies itself to the %TEMP% directory of the system and executes this copy as a new process. This new process performs all the encryption on the victim system. Before encryption starts, this new process first logs off all active sessions on the system. It then changes the passwords for all administrator accounts on the system, preventing administrators to stop the malware from encrypting data by logging in and killing the process.

The malware enumerates all files on the system, and for each file it wants to encrypt it launches a new child process to perform the actual encryption of the file. All encrypted files have the .locked extension appended to them. An important note is that LockerGoga, unlike Ryuk, hardly whitelists important system files directories. Even the Windows Boot Manager (BOOTMGR) is encrypted, which means infected systems can no longer boot.

Like Ryuk, LockerGoga uses a combination of AES and RSA encryption. Each file is encrypted using a unique AES key, and each victim has a unique embedded RSA public key where only the attacker has the private key needed for decryption.

After the encryption process is completed, LockerGoga disables all network interfaces on the victim system. Ransom notes are placed on the system containing one or more email addresses to contact the attackers on.

https://labsblog.f-secure.com/2019/03/27/analysis-of-lockergoga-ransomware/
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

4.1.3 MegaCortex

In the most recent attacks seen in this investigation, the attackers have started using MegaCortex ransomware. This ransomware family overlaps on some interesting points with LockerGoga. Both malware families have been seen using the same C2. Both malware families have a similar list of processes they try to kill before executing the encryption process. Both malware families also share a lot of similarities "under the hood", such as usage of the "boost" library for interprocess communications and using a parent process enumerate directories and to spawn child processes to perform the actual file encryption.

MegaCortex also only encrypts files on the system it is being run on and does not perform encryption on files on network shares. Similar to LockerGoga, the malware is remotely being executed using psexec. An interesting observation is that MegaCortex requires a specific password to be passed as an argument before it starts its encryption process. Besides the password, MegaCortex also checks the system time to make sure the binary is executed within a certain timeframe.

Where Ryuk and LockerGoga append the AES key material to each encrypted file, MegaCortex stores all key material in a separate file on the victim system.

https://news.sophos.com/en-us/2019/05/10/megacortex-deconstructed-mysteries-mount-as-analysis-continues/

5 Possible mitigations

There are several mitigations for the observed attacks and ransomware in general outlined in this document. The attackers use multiple methods to gain access to a network, which might require a more in-depth defense next to the possible mitigations listed. There is no 'silver bullet' that offers complete protection against these kind of attacks.

5.1 Disabling of SMBv1

Although it is recommended by Microsoft to disable SMBv1 for several years now (and even actively disabling it by default since fall 2017), it is still enabled on many systems. These systems could be used by attackers as a stepping stone towards other systems. It is highly recommended to check the network for the presence of SMBv1 systems.

More details can be found on:

https://support.microsoft.com/en-ie/help/2696547/detect-enable-disable-smbv1-smbv2-smbv3-in-windows-and-windows-server

5.2 Whitelisting of specific code signing certificates

With any default installation of Windows, all issuers of code signing certificates are set to be trusted. Attackers actively use Code Signing to bypass endpoint security as they treat signed applications as 'safe' and/or 'secure'. With over 558.000 signed malware samples in VirusTotal over the last 90 days (measured May 22 2019) it shows that this trust should not be enabled by default.

Additionally, unlike SSL certificates for websites, a revocation or expiration of certificates does not have effect when executing malicious code signed using Code Signing. Tests have shown that in both cases, malware not only runs, but endpoint security still gives the same level of trust to the signed binary. However, same tests show blacklisting the applications certificate (or its issuer CA) prevents Windows from running the application.

Using Active Directory, all known certificates that have been used maliciously can be blacklisted. By moving these certificates to the untrusted key store, the applications signed with these certificates are no longer trusted. As these are not trusted, Windows refuses to start them, even when the certificate is still valid.

You could also block the intermediate Certificate Authority (CA) used to sign the malicious binary, which blocks all issued certificates automatically. Each Certificate Authority uses a specific intermediate signing root for code signing. By moving these intermediate CA's to the untrusted key store, the code signing certificates issued by these intermediates are no longer trusted. Organisations should take note, any applications used within an organisation that have been signed with certificates issued from blacklisted intermediates or CA's will need to be whitelisted.

More details can be found on:

https://docs.microsoft.com/nl-nl/windows-server/identity/ad-fs/deployment/distribute-certificates-to-client-computers-by-using-group-policy

5.3 Whitelisting applications

Tooling such as AppLocker allows end users to only access applications approved by your organisation. SRP can also be configured in the "allow list mode" so that by default all files are blocked and administrators need to create allow rules for files that they want to allow.

More details can be found on:

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/use-applocker-and-software-restriction-policies-in-the-same-domain

5.4 Blacklisting unneeded applications

A quick and effective way to prevent easy lateral movement by attackers is to block tooling used by the attackers.

More details can be found on:

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

5.5 Finding Cobalt Strike servers

In all known cases, Cobalt Strike was used at some point. Therefore being able to identify these servers online and blocking or monitoring them would be additional line of defense, which is not limited to the C2 servers found in our investigation.

A server is running Cobalt Strike, could be identified by its default certificate. This certificate contains a specific SSL TLS fingerprint and contains empty subject and issuer. (CN=, OU=, O=, L=, S=, C=). Additionally Cobalt Strike versions before 3.13 can be identified [1] by an extraneous space in the HTTP header.

[1] https://blog.fox-it.com/2019/02/26/identifying-cobalt-strike-team-servers-in-the-wild/

6 Possible detection methods

6.1 Monitoring specific commands

As outlined in the TTP's, many of the commands the attacker uses are not used by an average user of the corporate network. Next to creating a mitigation to blacklist these commands (or only allow whitelisted application) you can also monitor the usage of such commands.

Examples can be found on:

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/monitor-application-usage-with-applocker

6.2 Monitoring on SMBv1 packets

Scanning for SMBv1 enabled systems within the network, as well as monitoring for SMBv1 traffic, could identify vulnerable systems or an attacker actively looking for such systems.

More information can be found on:
https://blogs.technet.microsoft.com/ralphkyttle/2017/05/13/smb1-audit-active-usage-using-message-analyzer/
https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/smb/smb1.rb

6.3 Monitoring on mass scanning

Network administrators could monitoring on both networking scanning and port scanning of systems in there network. There are several ways to do this, such as:

- Monitoring ARP tables on systems and network infrastructure
- Monitoring for large waves of ICMP packets
- Monitoring logs

6.4 Running a 'honeypot' Windows system

An option for detecting is running one or multiple honeypot systems as a decoy or 'tripwire', however you might need to take appropriate legal safeguards to prevent possibly inciting a criminal offence. When running a honeypot, an organisation must make sure it is a Windows system and this system joined the Active Directory. For example, a Windows 2008R2 system could be used with some non-recommended features enabled such as SMB1.

You should create a bogus organisational unit (OU) within the Active Directory and reduce the trust of the systems in this OU, so when it is compromised it does not create a threat to the Active Directory itself.

You can monitor on attempts for ICMP and activity on ports 143 and 445 (and specifically SMBv1). Any other system trying to contact this honeypot should trigger alerts.

6.5 Detecting AD and local administrators group changes

The attacker creates new privileged users, and while it would be hard to correctly monitor new users, monitoring privileged groups is a more feasible solution as these groups are unlikely to change much over time. Examples are local groups such as 'Administrators' and domain groups such as 'Domain Admins'.

Examples can be found on:

https://gallery.technet.microsoft.com/scriptcenter/How-to-Get-Notified-of-5afdc4fe
https://gist.github.com/anonymous/028d51b9b5a16144637o985ef35e0c2b

7 Indicators of Compromise (IoC's)

Note: the IoC section in this TLP:WHITE version has purposely been redacted and sections on IP addresses and specific identifying elements have been removed to comply with General Data Protection Regulation (GDPR) as well to prevent impact on the still ongoing investigation by law enforcement agencies.

7.1 Software usage observed on compromised systems

7zip
Adfind
Ntdsutil
Net
Ipconfig
Netstat
AnyDesk
Wmic
Whoami
Powershell
Driverquery
Echo
Masscan
Psexec
Mimi (mimikatz)
Netsh
Nltest
Osql
Portscan
WinPcap
Mstsc / RDP
Nslookup
Ping
Query
Systeminfo
Reg
Process Hacker

7.2 Software usage observed on attackers infrastructure

CobaltStrike
Armitage
Metasploit
TunnelService
Hamachi VPN
Impacket
VirtualBox
RDP Brute
RDP Recognizer
DNScat2
IP List Generator 2
Phantom Evasion
SecretsDump

7.3 Observed Code signing certificates

Subject **CN=ALISA LTD**, O=ALISA LTD, STREET=71-75 Shelton Street Covent Garden, L=LONDON, S=LONDON, PostalCode=WC2H 9JQ, C=GB
issuer CN=Sectigo RSA Code Signing CA
Serial: 5DA173EB1AC76340AC058E1FF4BF5E1B
issued: 2/21/2019 4:00:00 PM

Subject **CN=MIKL LIMITED**, O=MIKL LIMITED, STREET=16 Australia Road Chickerell, L=WEYMOUTH, ST=WEYMOUTH, OID.2.5.4.17=DT3 4DD, C=GB
issuer CN=COMODO RSA Code Signing CA
Serial: 3d2580e89526f7852b570654efd9a8bf
issued: 06/25/2018 02:00:00

Subject **CN=KITTY'S LTD**, O=KITTY'S LTD, STREET=Kemp House 160 City Road, L=LONDON, ST=LONDON, OID.2.5.4.17=EC1V 2NX, C=GB
issuer CN=Sectigo RSA Code Signing CA
Serial: 378d5543048e583a06a0819f25bd9e85
issued: 02/01/2019 01:00:00

Subject **CN=PRO-STO, TOV**
issuer CN=Sectigo RSA Code Signing CA
Serial: 00CA0E7090D4827004C99AF2FC7D733C02
issued: 03/01/2019 01:00:00

7.4 Observed File MD5 hashes

These MD5 hashes are mainly from the CobaltStrike database, which keeps a record of all hashes used on the victim systems by C2. Some hashes have been added from other sources that have been found on compromised systems.

0037d678bc22c526b047ad4c6fb08722
00f1f58a42c2aa8205f6dcb33b4abf18
011319661454ff8625eee11f171f4d8f
019d43595b28807cc0c4a51671bf0a03
01eb9e99747b31e630846ce984238d0a
0213150a3ae89e15d8566f9f3f4467d6
02ca44aee715c8b91d3271b4f583edcf
02da841d3c9e690524784 56f585ed968
046e022f3c89b66a07b4bcf5acd47de5
0570684fa7ffceec4e429cb57227e2b3
06068b7b44cac25b32997bd9ed81eaa1
06457b317d56245908 03a77d3770bff2
071a87637a7b4e23574aa23f3d486bd8
0732159bf0992c4159dd9fb24ea9add5
07790b2c96e6ee1fbd4429aebab263cd
082e0edb491a2337bc25bb594a7d6a25
084b596ed3ed345e0be184587d3e2cf5
08c09677f1f3a5a00cddffd1307ecf44
08d7cb2781abcac7c58522300e41d591
08ee643bc38254edd4f1853f10008530
09409aac4f2ae21413fa45d84b136e1a
09feb5a72ce8deffcf3eb5f7cdacc8e5
0a04b55be225b3839813f70a4bcb1ca4
0a1f19818233c868860abe1a614d7768
0bdf6bc8afcbc83c7fafd9b0e9315aa5
0bfbfc5ce1288ab9c80d8c0466887b8f
0c539b67001e093c3a4b23d9de4a565d
0cd2cbcb8626332b5bff55b8e9ef6492
0cd8eb208a598ce1cfdb5659b4bdb8d1
0d0724ca2fabb55ee4db48c1ec33d8a1
0d52b751a24c10ab9d713134090 78903
0dcdf80b4b9043c6f23973e0826bedd7
0e37fbfa79d349d672456923ec5fbbe3
0f61fdf0b7862d20bc08513e38c14599
0fac645ea909a07f36b464f854c9367d
1057a77de8075755a4e1401a9f9e5f70
110b549b4cc5bcc4b97b274f95c5d2af
120a6c8b8c9e868df575d91a8060bb5b
1250bef11bfa086f772cd2a273bc036e
12aeabed146e88b97a4821ca913573ca
13ce5078f2d1b56d8f986b875e8aa3c9
15b9e2c753502e552b914f9ebdbb006d
15cac1afbbb09047de6e032d18a4a878
15eea35d1af5552f212824fd04dead09
187f10ce2588cc553c4a75bc47d018cd
190a9d5b3f5ae5c77f0da5cb26f3a364
196c58e91ddbd526b0b38811f72a1876
198c2b3f18dc6b30dbb5826a995bbf70
1a2ffbf708845cff8c313698294d96db
1b03a14c8d25f430e1514422e09dcd82
1b2b1c9e39d385ab607377ec2b7e7ce4
1bb8b3b2b9770185ffd95468555e9781
1d42b74d3c3ca90a3654c6432bb76f6e
1dc5de239d0c5f0aad7f7fee30007ea7
1dc78ac6fc99cd146f9fdad6ec095151
1e9b519e3f2bcf8475dd8a22e7ad1b15
1eb242b7d9f3c6dba84762ea17027979
1fceea1fce6930d934bc7dbc3fca86fe
2043a5be49916b0dc81a6abf48936e8e
20b8546bc70de4e09fdb1c f0f6c76f29
21422937e0107e063ea3e4d620346a8a
22345defbbc3cf00880b123f240d9456
224bd868686f649215cb3937aec79279
229f53e671281cb58417a4b30d12a90c
22fe497daf9bf4036d7ed5c9e78204a2
2392f5a0e68319bcb8360251ac787d79
2519dc87261ed950996c9108e0582d96
25ef39b827baaf72301ba1616 46f8b61
2649dd4a858d63d09569e33b10796c30
266686593b4b376300e8eb7344ad2495
267c815d4a560a8f9cc87d1283e9f375
2692cce20d8d3b9bc42171abbd599a5d
2711439ece5d6c46727a073fc87c193c
27304b246c7d5b4e149124d5f93c5b01
273438b3f9c73a242c6c7f848682c17e
27a4cf3ab46e8b28e4f7011bc8dfodb3
28147a525a012df54c664a81eb90aa05
282c6754405a220a9f40b5309786eab9
29035ff5d3f7de963e9b341b89ca97e8
2968276980359334 76bb4b64cdfbf8eb
2994377903e3e993f70732b384711 47c
29b730896cb17761da86d80760b86b07
29de476d00f2ed506b64704f80181 3a3
2b09b469cfeddb758c843eb2a84be336
2be27964868f3ad85fe6fa2f03fac825
2c20526oc0e4cdad4005d77fdf7cc202
2cefc8024da5c59b45f78bebfa4ed7cf
2cf147e1b7891c1fbe8840d48f9bbf92
2e19640889cc1ee3a7cd78cac78a6414
2e6efd58d0b64c20962ff3219ff004d7
2ed5e2decf83a5959ce5d5f34dd9ed61
2f2fad1372b94ab9d7f701859f5f080f
2f39428420bb47f979223a681449ada2
2f556529e39cb3dedb19coba8e049d7a
30f79b6fa14e2a6aa4a64d057a19d8do
3103671de5a5c3aff128d44c0483f5eb
315f9ad98824f548bda229db5affd3ce
321196686ee96151ce89bc96ff53bd27
322d28b30c41e3f54548b94585a673ca
322d892fa02032ad6f4be582378ob357
32523c6ff6ab2844289d31a96e656dd9
326919c8625673860cf439ead18067e1
32eb92540bc948176621d3e6dc88bbf7
336bc2a46923d2d192f13853aa4foc5c
34187a34d0a3c5d63016c26346371b54
34b6440509013584 8db8b817a617efcd
3544d810cb8f5ee56ebceeoe246391b6
37eco16a897864e863297c41a1500769
39790e68e69f4828dce1749bfba2578d
3a2d02f07fda60143667of3acb2e9dea
3ac73275786243f06e81a045eca6b496
3b200c8173a92c94441cb062d38012f6
3c6230726d5811b8d58b3090129cdeo4
3do6d6bb4aca749e34afbb147a15d9bf
3dd2100179abd95574e1cfcb13025b53
40560d5633539b426ce32373cadbb9a5
407c22f9e38f20bb660788046e5136cc
40aef4887eb89c9660b3d1351b031a5f
40c20c0a00a5884fa4fob8e4c702b5d9
41084d26d6ff954528d758b392aa8ea3
410946e256fbf1bb12c00fa6789e460b
414d7be8049e3eede2213dc8fd026b65
41582e148ecdfae8f3aa0a3ea998884c
4179b59669841d9344ea273204edd42b
422d0a1a6643dd3d3e88cbc44cb54a38
426a8fdd698715b727a7b6cbf36375b9
42badc1d2f03a8b1e4875740d3d49336
435ee0c88707591fed0b5f01a4b911c5
43728968326d661eab301cb7b2bbf8ea
44301219ab3251696312 2e800fdd1d6f
45587of8ed6d059ed10c77d0101208 15
455dc5fe61c26bbb0d829d3f0a5d51ab
456999c316526cc94fabfdf4cb2a8614
45f02a758b91c820c10d50cca091000b
46d75853419e6f84c795e608da519ce4
4731c177142c95641348256544 5f0957
478e08c05a645e1abod77c1bb1bc97b1
49b232d0fdc3dac5f6770230c3e713ea
49bf61c5ec02849579da573f9febd8d5
49e477aeb61d854e0e3ac39eab728c23
4a124bba28a1fc9cf3d474142b5ad5cb
4c60509f09e64b3f357036de5ede5e9e
4c914cef8e1a9a2abc3980c5ff2a355d
4d00051c1422562c01f26cad07087e0c
4d5073126864dfe0056ode4d171506d8
4dfef5e7978ef13e4201a3d0b1ac07e8
4fa05d5fc7c6f235eee2593b39fd7f3d
4fd56e461aef6b2093ef8a5a3d11ab36
4fe37a4073687a0a522eb8770e756b5c
5067726 4a120f2a1e69b90620b8c6bco
506d8da34eefodb47cf47e5acc277fc5
50bbb6a056f4d8a3364c2becb679c0ea
512a1794dbof611a8906d3b3a07e08ee
514d2a5b4bbf5611fb0d9564ad8e6fff
51bbe74437f307eefa2a485c8e1763c8
51fb7a6bd2895595570 1deffbd2f3963
5270e39d11d9fad1de9bb5ae319330bc
527def710cecc31af233a0a3366109ff
528826cd6284be80ada59afb489ebeb3
538bb5ca41f6d6b42b763661261b1a19
54fc951fae5b3d6930cf1976d47797of
550c89b0eac5a81612678b167e8ed741
5553cafa15a222718ocfa2839e591f50
56283558d0a275ada8eef12a53e0447a
56469f4714ab4a94ba829eca635a717f
57c0c931d805809bfe9453937f16ab9e
5841890693f26e1445725594 42c4d526
58fdfffc409d04ef25e7c58a276b4475
594af71e693ea667fc95db990e3e38d2
59a432a683398ffd7506dddb2c35092a
5a572b98289054 9ddd1da84dbaf38057
5ab6b24be710758edc0bc7d33e1fbcbc
5af2ff9f4833c1a621990 4658ec18d1a
5b510339e89316 4c5a94c40d486c78ba
5b726399a3736eccc7f5339a67dc4abb
5bbcc3ed7c3f8a6f4c6cf82d3554d1db
5c5561185a875171115693 4585f002e8
5e4da000d8fc98482b2c5830d7159ef1
5e84ced3c031d48ad879f3afa89d3812
5e926ee9f721751b5c626d31be334594
5eb40fdf6d9be043f1beecaaa79028d7
5f7632a9118dc20bcfe6a6babcfc46e5
5fdb1138faf59d85fcf77152e7786dda
60562d05df9a92e7796d958a89e5c579
60ac8ea5fbbf9fa0c52f72f57f67d5be
610150d813582c4946a6cdb6fcdoefo8
6105e9697cfa0b0a3a73791a39c28142
61f2ac54c2c03aea671ca43cd27ee6fa
622d21c40a25f9834a03bfd5ff4710c1

628c2b376373a034805ce9b1009a6eec
63893fad3f6b1c69925e333c293b542b
63a9898eb31e210418b730f8cc8da8e7
643e7195ff5ea83e6d123759a35d693b
664c916a686e7403fc9ff66fb55d70b5
66c239fb53e79a533af2c1d2de63660d
66f93d6d5aae6ada544dfd5403a665a7
68598716obce368cod0269e9d6b85618
68cd777c01ebd505994cca9e4fae26c2
68d172f4a851433ae29ba11143a4b606
68d9cf76292cc1dbc523191235d08790
69d20bc54e61557e372c64d263a4e994
6a3583d763bc41d4363cf4acf85206f8
6af4703e842a0e451c8634e363c09f39
6b3fd11f65d88dd168126de17d9b77f6
6b40ffc7d8d28c47af641a75a08ccc2a
6b90a6cffob9876bdaa37052d16db064
6cc00b3be6160257cdfd9b228d758337
6cde824a970c08629d82ba36767cf4ba
6d1bf694b2839b74db2b4d6040fb6b3c
6d6bcae3bbfa65409e1bc183ed91f22a
6e4dfa932f836da1edb3764335bd2cea
6e8698452c4cc3df0053ff5783b4eb27
6eb45fe77cfda76ea469095ecaccf3e1
6f22d9cfcec4b7974d1a635ceea6f3e3
6fa813c93cabb5521e9896505127ab35
708e277cfd221a1adab5aa18eb6b1bd7
7184f48d43c583240731ae185bd74a8b
718b8b69c7ede1f34e83cc502b027c2b
72ed52edf85641d0d507690509913373
73d649bde2a3c8b66d0657b1759ac02c
7455b58281e695c63539652f4a56595d
746826c28b26fa98254374c06919f100
74b2b38684f1138a152219e3974a7d3d
74fb9fe012582861 1a24da0ab452c8904
75669ecc061fda20fd9aaa3b5b78c612
758db76db49fb81693cbcb48e941a2ca
7786d40a0a747b935f34a9a2d362ff74
7862742cda05c419b59dbcf7f1d42338
79ba0c5b9fb086cf3ecca3318785ff49
79ca49528861bea404dc3326260d8a72
7a7aa50e713be9316c9f48424b6b4eec
7a98acc8ae620c18edd5d19cd07111a8
7b3eba5b5b964e4624d1f8b1173f8c92
7b7a8436acdf7d277715527e9a8df316
7c2cc2519c5782da2d9cf8b08ed6ce04
7cd034bbf9c6ca27ddb3f806d6234923
7cdf1e926c62115137 10c56534201f85
7de9508add93f9d1752c148b69d5f9fd
7ef73e04190c2c76c771830f2121f158
7efe3bbd596fac45546d0e208355ad3c
7f8494846ed03f1de302e31166338562
7fef8e91e666195fde16fcc60da42a78
809e1a5da528dac68b537d41474b094e
80bb0736ae33b5ae900edaef4deof2cd
8156350e1fedba3f07d0967d33804d87
81bf655ac72b3cdbf61cb7d5c48c074e
825eb80e2a9caa93d872b41eaf3e5134
8331155b9dcb17bc8d5c06888b2ed1ce
83430198c991fb67f2e1e998a79ac364
837ac591ae28foae4ebca87e9e85467e
849a95c0a19b8foe6c1fdb8adea05c51
856459ed52e4976072 7468aa7263b8a1
85898c49a3f9ce6b3df4b607a85f2085
860c1508065ba952ea47ca93ae682c09
862fa7430f8a6d32caf227ea24904a75
86fed2ecb1b581f8e4f722b6df22096e
87084ffcc536e5476afca0932f3c9ea8
877b527bcb75997d6b18900f7eed49d1
87b4d95becdee0aab49bd7566de83804
885646ceb21d4e68cf3176 4652ddaeeb
8898f013bbce6d9df4946afe81609226
89079afoec13de3310ad4e55ce0e0b93
89bba7273b4089517b4fae06574f5550
8a5174556abfe2806ce23d5b27d4e775
8aa94d877cef6ecd84fc1bb906e4e569
8ae3764b69e76a4a225c90540a1c1f1f
8b0954d9c76974a30cde373f9d5b833f
8bd8153128bb14750e2b1f2e8d5e1282
8c154999c5485797159afeeoc2ee3bfd
8c3db475e02f7a8548546o6deeb88fo7
8d2c4b114502d6718b02d51d897b71db
8e3caed3e9182797fb561db237367446
8e54fc99d0a0cc2a791dfd06695b8739
8e5foc7dab20e34fe3b93793522378a3
8e9e9651b687b9042c2e7d3bbaadf643
8f1dc5e2ffoe365b8921059f8843bef9
8f2245dac184d9065471 0526e2eda27c
8f6dc871498e65694a2b88841c257afb
8f9dfb1beac956691de59c233dc5ad96
8fb3b6162fd8a7a4db54ec908df81262
901f4621edaa39a6e64e7ac119beff23
90a18bac2a69d66722e6f8ea18d9f45f
90d288b10ba2099ecfa361d5edaea1d3
90e8cf58aa611ad9d9a0d9820c24e136
9141d75bdafef0071b329d62a2d1bbf4
92786138d979ea0f09dbf4fa1778e557
932fa8d5d3c5bae1bbbe26b30fd9c855
93dcdce62bd979ccf978b92afe5352e6
9441boede6c6cdf6c824bed90395d9f4
94601116b78ab19efb78c0814fe14255
946abdbodf46a90b440d5a5ac1fc7b9e
958291039ba5e50ac738504a4c1f3956
95a3a31e3ab597acd1552b689ec79468
964adc8794dcf4bb208ea923ddda71b1
97122bdde07eaaeeb2606f14c6564 12a
98ab50267b2bcb22041644ef897d82ab
991d0957b8e9eb010918d8972a5a0984
9936378a62 41e88e47d4f1f4aec4973f
994f5dd4a301287baeb53d4541f1fode
997177aa301d5doab06f3ba0bd38fcd8
998f096c04cbeddb8c343fcdb6a202d5
99a506957abe383987d5023d19c23f1d
99f7a5b927b4321ffb365ef09340c2af
9abdd71c8e6500528df56680d91063f9
9b02dd2a1a15e94922be3f8512 9083ac
9b33e1b340df35e3eba7bdf2eebbd980
9c3af41ca23d7ecaoe3d08e431b1bba4
9cd9f16432e5e6dcf89f70394abde277
9cdcedfd2045e5dddc33f556ee26964e
9doc12f719758d7f68cbbd2b65c75b66
9d2add922a5136cb0aa8eff6bddc31cc
9d3fdb1e370c0ee6315b4625ecf2ac55
9d61e34eeb98ef4odofode5b7fbd4od7
9d94e47b8d4a59840db8de90d2aa6a96
9dd5141aa95962c61d2a98e8cf9916a1
9e58805050b374c14ad3dba19de66ae9
9e79d3f77b468232159a79e91578b970
9eaf1ab5ef4eec6e9783a95ea515fdff
9eb427d27938966753c38928831c3bbd
9eeed1dc8974e4352f2627362027a8e6
9fd521be4c49a1d361399ab732f33074
a03c6551d67ac49092d972e864fob788
a0492d5798944264ca83968927b1b18f
a070ced0e86ffdf7cb81d4e9f65d4a51
a0c551398a51376b425dfc1d90ea7ed5
a0f919beee3e8f6bf2afa150dc6bce32
a12f1dacc962cb77fcfb3024b567a6e2
a13f2ad6129ea1846a0b87d990294 61a
a1f17b6b97b06356019d0205bb05e922
a3a1ce865a4434d8540269 1a4086a815
a3a93c06043b3a5d8b04eaf67075056b
a48bb767f15512de4f501a43f6714cc9
a49374eb6b586d892b30cf4079514 20e
a642f02cbb7995c4c3f5b19121e78c95
a6a1a80f5312c9e68afdee6070c5133a
a6c5bcc3d38a38582445ecf74dd63567
a6dd553c9c7af02e57def5604e2bc548
a7b43ce8bcc5cc09dd4dde35c6cba53e
a7b96bb0847b26dde3e4f1551228efe7
a81450136dd7eec021eb15298a97da03
a881811d22ef75196ba404798a494071
a99a178872 3e58f6568e278ce388e294
a9a316053c11d830dd8f3eedb3614e6b
aa062e951d4ff50e4250a4f3eb789a90
aa9f00481a3846aa2a9c752d0f7f637d
aaaa7316c3860a2ce2013c24f4a909dc
aada38a491183c9dbaf5fd1312202016
ab00a170c2631fd768f5c259a7948520
ab5d618c2fa981ff3380b10169724695
abcd7bae6ce320dc52b798eb1foea13b
acc61ad027de93338143b4f4259ccc08
ad547716ccaf640888abb6ed4a4a81eb
ae578937e0dccb25c31276d6a75dec6d
af42d70747ea96d456101a67587b1b5c
afbeb0d4ff9851009000d2892afe133cb
afef6afbec1f95f86c7f35273e99b12e
b002217df8e44c12a24cf68aa57431c3
b1f7e8159da72fc850cc9baac4951bec
b2f28c3ab71f5350c96ec987f67b18ae
b2f54ed4bddf3a8f15bd65c3f7437b19
b32863d673fb83747add47ff405a677a
b3f7ae60bc1c08659990e412aa4e3398
b4998f95a0a7eb363b17d719b7f1c1cc
b4b6654e3a349c8efde0a0781c72b05e
b4cc9631edccbcfaf04a1d99e8a53ec8
b50dcfd171f5ff1bb0c5609720f68c78
b5183500274 22f2ab699c09719ec160a
b6f58661cfc5073053634cf0374 60846
b767a65a01af28a0fa0c467c014474a6
b7b9cfb013ab9a57f8ef439da636c7ac
b83a2e832a288bca3d3a2546141e74b3
b85a7e7b4ba6c21bccd653464c3cc950
b8c50c8065537eb0152e1241f9f8c9d7
b8e9efffb70c1ac298007fc42f7b4deo
b8edof25e264a7ec4ad2e32940efb4a4
b91c07ef9d7b77b6aec96dede21c14f1
b94d355ab73046a69bfdf74efb32e258
b99edac760734ee793a71b51569e209a
ba3a7861f7d269a73f6ee509b6466290
bb64fca9bf34c0673127c58d7218b2b3
bb8f4b4929c0303954b3d92258cc9ef7
bc3b71050oee6e41b34e8face4da37cc5
bc576a142e65cd3c1860bab2f6d00cf5
bdo4ddefafc6574bc9319ebb74f2633b
bdbf1a8dd567e75ecf7a60ddc35ed5aa
be4170ab9b3a35beccea6d42515b1007
be67d91b6b9d7eb38acf4e07d868e9b8
be81ed2d6605773b1e93e04e6ace50f8
bfbfof15dc59c25234e45517fod5d88b
bffcedod447ee8d48b473a47ec667f58

c035e4aea7714b54b8a26ff9256f5e64
c085f99990ad9ae518c014feda07e4be
c0a2cda29866d7bb0f21f762a5fe60e7
c16326f0a036d2bc47a54d9dc2f23f9b
c18064cda4f4e022c721d6a71c2c9955
c1ce5a232f00bd8a45f271958dbe1e56
c36a58966754af45af2cbf98fe317697
c3e78c8be16e9ad6374026d8bc97ea7b
c40edef455ec6b0cb1823f979643e371
c44d6f462338b26098ab9a1292005 3a4
c46cba8db47e954db86f56c5bacf6987
c4d4f1391e8f2b0e55e6b7b72423e851
c50de2f01665241dd5aaa805903a3021
c50f3b0b23dfe5c66561bb9297bf7bbc
c56e8525756a89ba7d724564840ed47
c5d2a6dfda0976a0e120febebf8fad6be
c691d2c20ff15a36b93be5fe31b1a327
c6aea0542bbd71f589b651b7ecce8d39
c6d112937e091a9addb6a3904ca4cae2
c6f76b06716c540b88fbaa0aeb0ee339
c707800f439a14585fab1ab81283dc0b
c7baa88b92609c661bc6aeaeof309aed
c7cc3fb6b0af21de9ab17407135b0f6e
c7fa5301e528909166 1a71881c9d743a
c8bb0f4b569ea79827439e28e7b02839
c93b8f6950a4f39b4e2a050bd69f126f
c9b015706d74450822bbb6cc8caa3892
cac908841d5549f4cd44373f385e2dfe
ccbb3678a54897f1207f609c61901ea9
cdaa76c8a904fa1693260a53127ed0ef
ce0eaabe28ac18434c4402add075b5c1
ce1b96bf305cde596827906b31d7016b
ce5650d4c5b0c24f27a93859adca3e86
cef1360a0b46f917de375780afb8b8cf
cef33ac34d33d80312720845c4751c7e
cf04804d1cd24cfecdc39781d02a81a4
cfc0cf759f237912f5962e92b014fb48
d03b07b967e18209aa6cde3694f3bcd1
d0e3e57ef0b29c43a1fe4e358f8c16d7
d0f2ba1a6434856e9aba5de4407a1631
d18f15c85f9d51ccdeb1b617aed04063
d278a73b8b9b7583200168 31d02ae4a7
d55b59b94c8cfeb471608e9a77ede4b3
d5f37130f52be4550f931199d8527e74
d778eafcd7122695dcda760bef1d0ode
d7bee13d352853e242931c220dc9bc9f
d8914963afac09e3da3be2ba6a8e2e92
d95dab779bfbe4b4c4bed710a0ed1cc0
d98050f42807e24054dda53349fb3899
da11b1fdd11548b3bf529464544 94dd0
daa2e13a85da2140320866b289cd9e9d
daacda27a11e85e6286195f041c8b4ca
db01a6a1610b91f633df16b276b73737
dbce107bd068d3091770076 5345a05fb
dd5c69659fa7b8b3e4ead48d69572e3d
dd9d25fd76d0a0c174ae4ed9057d0c0f
dda25c9754d351fae6239ceca11719d6
dee33001d552ab6d9830a430b854eb61
df21972142fbff5e73dd17449c8b7caa
df5ce1159ef2e257df92e1825d786d87
dfe8b5e05eb9de766d91342adc065841
e07272c140b9d4a36ff2418e44d20579
e0ab5c98243793a34aa94dccf1f6ad57
e11502659f6b5c5bd9f78f534bc38fea
e1277dd2670daeb7814275d958872a25
e1626fd4009e27fd288c6d7d3dc687ed
e166d7ed4a97904d81deaf2c4ad35be6
e1ecf792f5f335e12aefffc1d8d5f396
e2eeb2659f00374e184ec2871f31836e
e38ec974fb71c2085eafc81eedd19751
e39707dfb867b08f768538c28fec2ad5
e4f76d92e66a9d19fe3997f431b0be0d
e50b384da6a0c0b43176062ddb6958d5
e59b21ce0db330dc8a7925a8835d3810
e5ab4243c5fd78a04fdf13da0f7bacb3
e5ba37ad46fdda013c48b3f781c67d6a
e5e37b12338695c09bd852a983720b0d
e649f788afa01ae23779c53074ccacab
e7230fafe4492ce461eb30a5ec087f7f
e84d7d638e09e9a7c8c8ef293d7dbdeb
e88e3e02e52dcd5d805af38274d37958
e91251fd1e2508b4111f39676b9d1f9d
e9c3179ed49ce97ff5b6301f7aaa6f92
ebf21603e6d87116dc42a8c4c7214dd7
ebf6f4683d8392add3ef32de1edf29c4
ec14598a2b7217d414dd010ad735cb18
ec14ccaff4773091d37e09ed49e9c550
ec19cea0fba30cc26013677d21351556
ec94b55ec8201236b9bf6ab7ff4e98e8
ed0c93ef5e8e1d3bf3dc1b01032d7d29
ed463b53594ff4f3375cafb6bf0d3073
efof497ad07de0d4d9d01df6d6e31602
efdab1f6326b57be84087ff71fde8eee
f16a7b7b8f356c43798ddc37af9f77d6
f1f48a305a32128554862e7e56781099
f222fa064ea00cc8369c413c277c8c16
f327ecad8304091fe3ebd046ea1e7692
f37f875b034cbd55d335e3eb9aea4d52
f41a1afc4cfb95f35cd92da98d90c27b
f4e5a845a1734d80c6f7066fad696d0a
f53797ee7f5fd13afeed39943e5cc793
f56a6de38b2dbc4e80adc9ad94f27cb7
f5ba35ef0e1c8598e6f7e1a1c783b7e6
f71c18fa089f13f41059344dff6568c4
f814070c59caa095d35a9a602bdd3a52
f84066bd7cb1aa0e3dce592235f12e24
f9f435cf0983dbe70da1503eab850d35
fabe38571a8ebd4deb11152d5e9d0ada
fbd97b2699ee67808e465da93f9c5700
fbe62f91b7612059c78cf0682a679ffb
fc3090322739504ff6b0a14468a9657f
fc36c490bd5e063c6808e5c822b22b6c
fca44db155ff7550aad6bfeb8dbdce9d
fd2e78aef78e02adcf6038535be75dbe
fd83e2265af3680717a6a86aeb381c14
fdcb4fcfba293b1c7f6955d42cb8d027
fe1692f4a6ac24012cef509fceea1717
fed76c47804baf745399a9f1de822e83

7.5 Observed File SHA1 hashes

We also found several relevant and unique SHA1 hashes on compromised systems, where we do not have the MD5 hash for as these hashes where found in log files on the C2 servers or compromised systems and we do not have access to the original file.

059107eb8a7af56cbc4eb3f4383ad4140a014bfe
78dfd4ece81d71a9c1d49909119e12da9cc280a0
8b44eaaafbe4be0f850d55841a7ada820900632c
ee9fb2b9a56fea7a51819a5f3a7b928ce2082a05

7.6 External public sources for IoC's

Based on OSINT we can find several additional sources of external investigations done on the same infrastructure, which we can link together based on IoC's and/or TTP's used by this infrastructure. IoC's from these external sources have not been included in this document, though they might overlap.

- https://www.abuse.io/lockergoga.txt
- https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html
- https://news.sophos.com/en-us/2019/05/03/megacortex-ransomware-wants-to-be-the-one/
- https://news.sophos.com/en-us/2019/05/10/megacortex-deconstructed-mysteries-mount-as-analysis-continues/
- https://github.com/sophoslabs/IoCs/blob/master/Ransomware-MegaCortex
- https://cert.ssi.gouv.fr/actualite/CERTFR-2019-ACT-005/