CosmicBeetle steps up: Probation period at RansomHub

welivesecurity.com/en/eset-research/cosmicbeetle-steps-up-probation-period-ransomhub/

ESET RESEARCH

CosmicBeetle, after improving its own ransomware, tries its luck as a RansomHub affiliate

Jakub Souček

10 Sep 2024 , 25 min. read

ESET researchers have mapped the recent activities of the CosmicBeetle threat actor, documenting its new ScRansom ransomware and highlighting connections to other well-established ransomware gangs.

CosmicBeetle actively deploys ScRansom to SMBs in various parts of the world. While not being top notch, the threat actor is able to compromise interesting targets.

CosmicBeetle replaced its previously deployed ransomware, Scarab, with ScRansom, which is continually improved. We have also observed the threat actor using the leaked LockBit builder and trying to leech off LockBit's reputation by impersonating the infamous ransomware gang both in ransom notes and leak site.

Besides LockBit, we believe with medium confidence that CosmicBeetle is a new affiliate of RansomHub, a new ransomware gang active since March 2024 with rapidly increasing activity.

In this blogpost, we examine CosmicBeetle's activities during the past year and analyze the connections to other well-established ransomware gangs. We also provide insight into ScRansom.

> **Key points of the blogpost:**
>
> - CosmicBeetle remains active in 2024, continually improving and distributing its custom ransomware, ScRansom.
> - We provide an analysis of ScRansom, emphasizing that it is impossible to restore some encrypted files.
> - CosmicBeetle has been experimenting with the leaked LockBit builder and has been trying to abuse its brand.
> - CosmicBeetle may be a recent affiliate of the ransomware-as-a-service actor RansomHub.
> - CosmicBeetle exploits years-old vulnerabilities to breach SMBs all over the world.

Overview

CosmicBeetle, active since at least 2020, is the name ESET researchers assigned to a threat actor discovered in 2023. This threat actor is most known for the usage of its custom collection of Delphi tools, commonly called Spacecolon, consisting of ScHackTool, ScInstaller, ScService, and ScPatcher. In August 2023, ESET researchers published their insights into CosmicBeetle. Shortly before publishing, new custom ransomware we named ScRansom appeared that we believe, with high confidence, is related to CosmicBeetle. We have since found further reasons to increase our confidence of this relation and believe that ScRansom is now that group's ransomware of choice, replacing the previously utilized Scarab ransomware.

At the time of that publication in 2023, we had not observed any activity in the wild. That, however, changed shortly thereafter. CosmicBeetle has since been spreading ScRansom to SMBs, mainly in Europe and Asia.

ScRansom is not very sophisticated ransomware, yet CosmicBeetle has been able to compromise interesting targets and cause great harm to them. Mostly because CosmicBeetle is an immature actor in the ransomware world, problems plague the deployment of ScRansom. Victims affected by ScRansom who decide to pay should be cautious. While the decryptor itself works as expected (at the time of writing), multiple decryption keys are often required and some files may be permanently lost, depending on how CosmicBeetle proceeded during encryption. We go into more details later in this blogpost. In keeping with our experience regarding CosmicBeetle, an interesting study of immature ransomware groups recently published by GuidePoint Security shows corresponding results.

CosmicBeetle partially tried to address, or rather hide, these issues by impersonating the recently disrupted LockBit, probably the most infamous ransomware gang of the past few years. By abusing the LockBit brand name, CosmicBeetle hoped to better persuade victims to pay. CosmicBeetle also utilized the leaked LockBit Black builder to generate its custom samples with a ransom note in Turkish.

Recently, we have investigated an interesting case that leads us to believe that CosmicBeetle may be a new affiliate of RansomHub. RansomHub is a fairly recently emerged ransomware-as-a-service gang that quickly gained the public's eye when Notchy, the notorious affiliate of the BlackCat ransomware gang who claimed responsibility for the attack on Change Healthcare, complained that BlackCat stole Notchy's ransom payment and will therefore be partnering with the rival gang RansomHub instead.

This blogpost documents the evolution of ScRansom for the past year and CosmicBeetle's approach to compromising victims. We also dive deeper into the threat actor's relations to other ransomware gangs.

Attribution

We believe with high confidence that ScRansom is the newest addition to CosmicBeetle's custom toolset. In this section, we explain our reasoning.

ESET telemetry shows several cases where ScRansom deployment overlaps with other tools commonly used by CosmicBeetle. Additionally, a ZIP archive uploaded to VirusTotal contains two embedded archives, each one probably containing samples from an intrusion. Both archives contain ScRansom, ScHackTool, and other tools commonly used by CosmicBeetle, further supporting our suspicions.

There is a lot of code similarity between ScRansom and previous CosmicBeetle tooling, namely:

- Delphi as the programming language of choice,
- IPWorks library for encryption,
- identical Turkish strings in the code,
- using spaces after colons in strings, which earned the Spacecolon toolset its name, and
- GUI similarity with ScHackTool.

All of these similarities further strengthen our attribution. Although Zaufana Trzencia Strona analysts recently published a blogpost about CosmicBeetle where they attributed CosmicBeetle to an actual person – a Turkish software developer, ESET researchers don't think this attribution is accurate. That attribution is based on the custom encryption scheme used in ScHackTool (not ScRansom). Specifically, they found a malicious sample (SHA-1: 28FD3345D82DA0CDB565A11C648AFF196F03D770) that contains this algorithm and is signed by a Turkish software development company VOVSOFT with a strange-looking headquarters.

But the mentioned sample does not belong to VOVSOFT; it is actually a malicious patched version of Disk Monitor Gadget, one of many products developed by VOVSOFT signed properly (SHA-1: 2BA12CD5E44839EA67DE8A07734A4E0303E5A3F8). Moreover, the digital signature was copied from the legitimate version and simply appended to the patched version, resulting in the malicious sample apparently being signed, but not having a valid signature.

Interestingly, ScHackTool's encryption scheme *is* used in the legitimate Disk Monitor Gadget too. Zaufana Trzencia Strona analysts discovered that the algorithm likely originates from this Stack Overflow thread from 13 years ago. Since the author of the post, MohsenB, has been an active user of Stack Overflow since 2012 – and, based on profile pictures, is not the VOVSOFT developer himself – it is likely that this algorithm was adapted by VOVSOFT and, years later, CosmicBeetle stumbled upon it and used it for ScHackTool.

Initial access and victimology

CosmicBeetle often uses brute-force methods to breach its targets. Besides that, the following vulnerabilities are being exploited by the threat actor:

- CVE-2017-0144 (aka EternalBlue),
- CVE-2023-27532 (a vulnerability in a Veeam Backup & Replication component),
- CVE-2021-42278 and CVE-2021-42287 (AD privilege escalation vulnerabilities) through noPac,
- CVE-2022-42475 (a vulnerability in FortiOS SSL-VPN), and
- CVE-2020-1472 (aka Zerologon).

SMBs from all sorts of verticals all over the world are the most common victims of this threat actor because that is the segment most likely to use the affected software and to not have robust patch management processes in place. CosmicBeetle's leak site is, as we will demonstrate shortly, very unreliable and

inconsistent; therefore we refer to ESET telemetry. Figure 1 demonstrates CosmicBeetle's victims according to ESET telemetry.

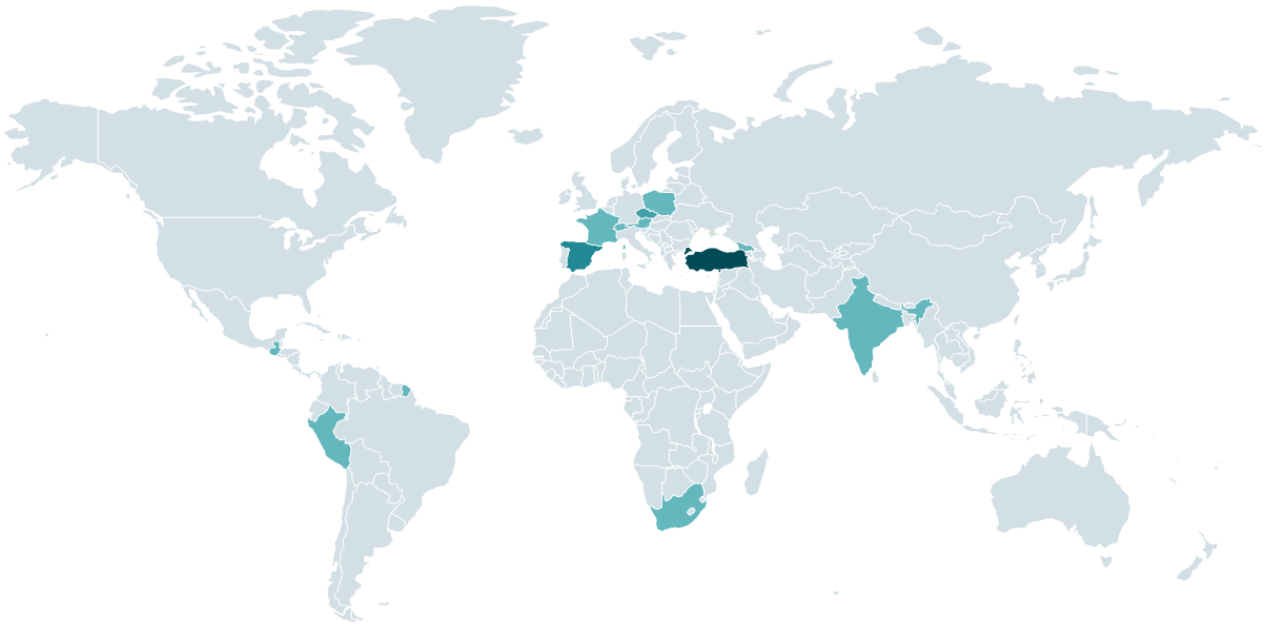

Figure 1. Heatmap of CosmicBeetle attacks since August 2023, according to ESET telemetry

We observed attacks on SMBs in the following verticals:

- manufacturing,
- pharmaceuticals,
- legal,
- education,
- healthcare,
- technology,
- hospitality leisure,
- financial services, and
- regional government.

Brand

Most ransom notes dropped by ScRansom do not assign a name to the ransomware. CosmicBeetle relies mainly on email and qTox, an instant messaging application utilized by many ransomware gangs, mainly due to its usage of the Tox protocol. The Tox protocol provides peer-to-peer end-to-end encrypted communication.

The only name CosmicBeetle chose for its custom ransomware is, ironically, NONAME, as the threat actor briefly branded the ransomware, which we discuss in the following section. Due to the chaotic nature of the branding, for the purpose of this blogpost, we will continue to refer to the ransomware as ScRansom.

LockBit copycat

In September 2023, CosmicBeetle decided to set up a dedicated leak site (DLS) on Tor, which it named NONAME. This site, illustrated in Figure 2, is a rip-off of LockBit's leak site (see Figure 3).

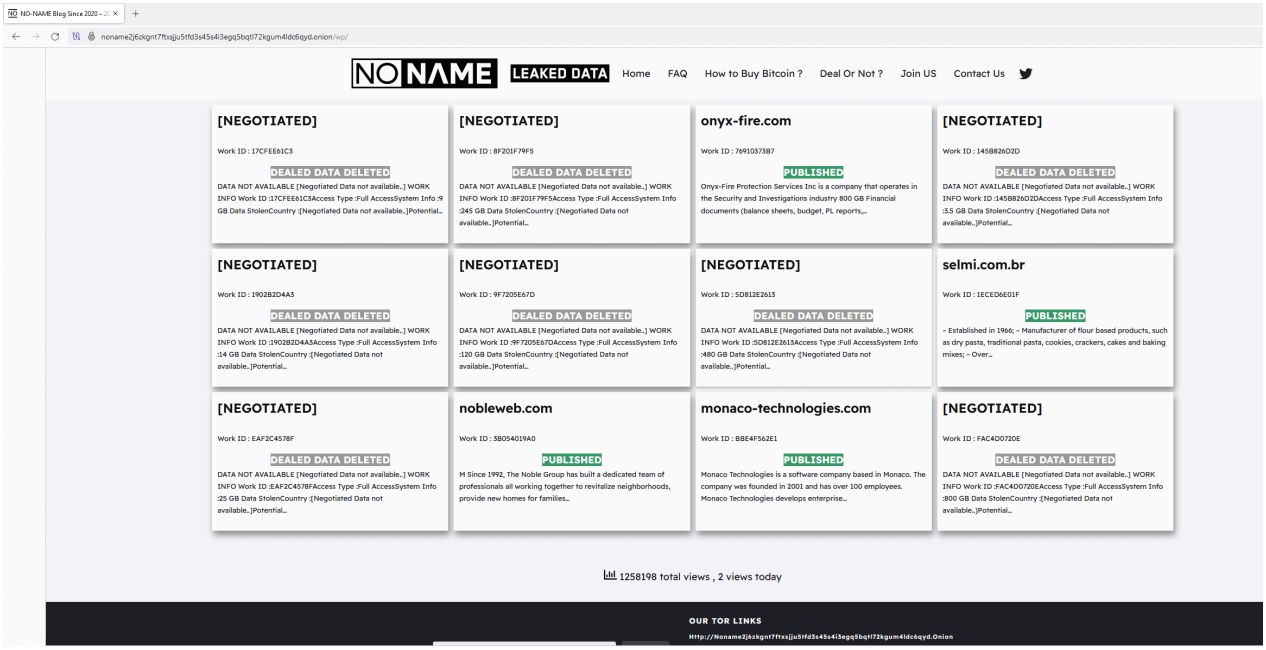

Figure 2. NONAME dedicated leak site on Tor

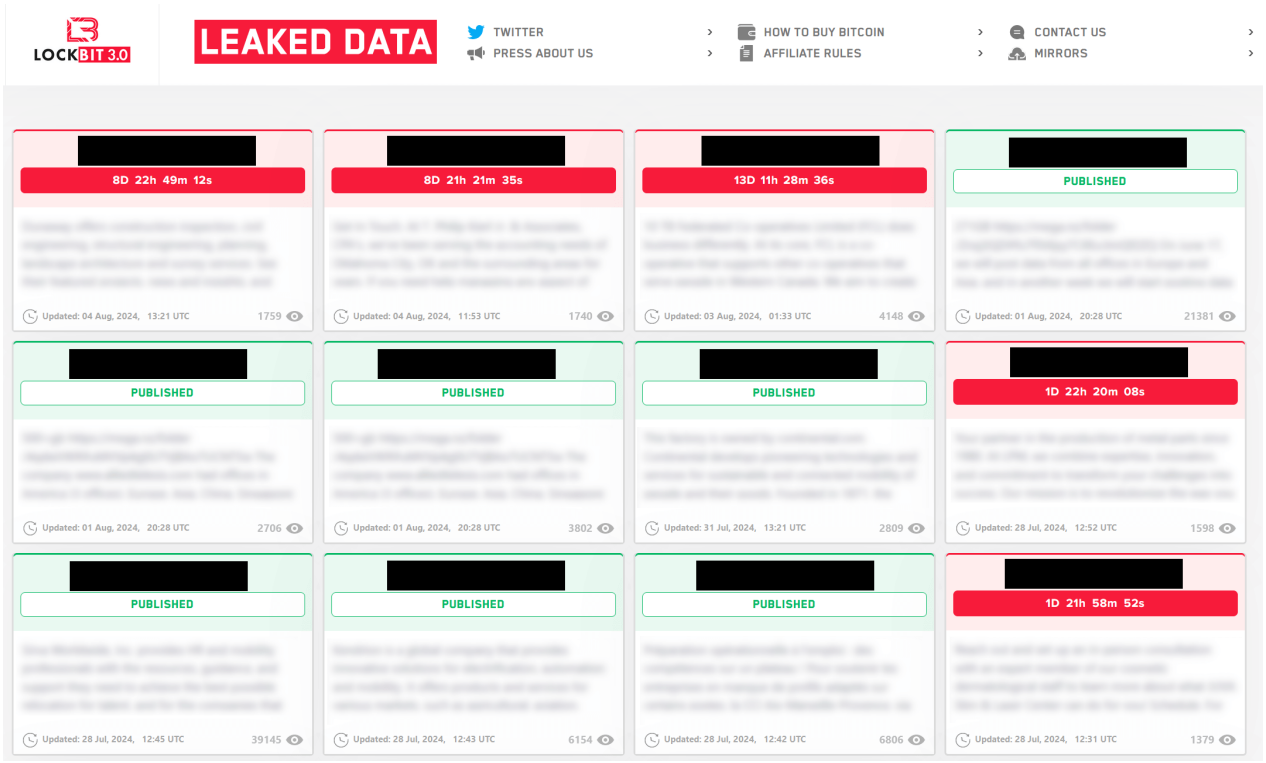

Figure 3. Typical design of the real LockBit dedicated leak site

While a few graphical changes have been made, the inspiration is still clear. Moreover, the design is not the only similarity with LockBit. All of the victims visible in Figure 2 were actually compromised by LockBit, not ScRansom. This can be verified by using DLS tracking services, such as RansomLook. All of the victims were posted on LockBit's leak site, most of them in September 2023, shortly before the NONAME DLS appeared. The Work ID string is added to increase the illusion of being related to ScRansom, as this is how victims are identified in ransom notes.

In early November 2023, CosmicBeetle decided to move even further and decided to impersonate LockBit completely. They did so by registering the domain lockbitblog[.]info and using the same approach as for the NONAME DLS, only this time, they included the LockBit logo as well (see Figure 4). Then, for a time, ScRansom's ransom notes linked to this website. The same inspiration is visible and the graphical similarity to the NONAME DLS (Figure 2) is undeniable.

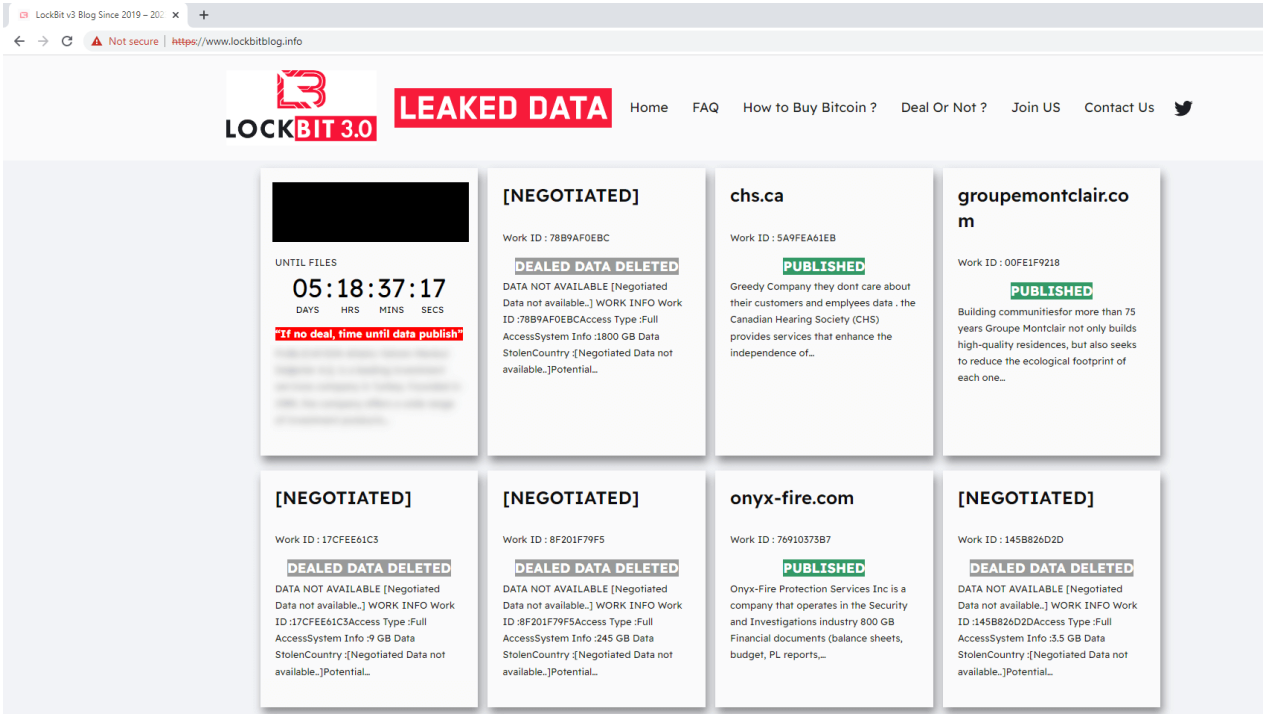

Figure 4. Website mimicking the official LockBit leak site, set up by CosmicBeetle

A sample built using the leaked LockBit 3.0 builder was uploaded to VirusTotal in August 2024 from Türkiye. What makes this sample unique is that it uses a ransom message (see Figure 5) in Turkish and the qTox ID it mentions is one we conclusively linked to CosmicBeetle. ESET telemetry corroborates this connection, as we have investigated a case where deployment of LockBit overlapped with CosmicBeetle's toolset.

I have encrypted your data and for the fee you will pay, I will reconnect to your system, decrypt it and deliver it to you.

We would like you to know that you cannot get your data back with known data recovery methods.

These methods will only cause you to lose time.
However, if you still want to use data recovery companies or programs, please perform and/or have performed the process on their copies, not on your original files.
Corruption of the original files may cause irreversible damage to your data.
The originals of your encrypted files have been deleted by using a random data writing technique.
Your backups have been deleted by writing data on all the backups in your NAS Storage and Disks.

If a return is not made within 48 hours, the password used in the system will be deleted and your data will never be returned.

Your disks are encrypted with Full disk encryption, unauthorized intervention will cause permanent data loss!

Do not believe the computer guys who say they will not open even if you pay them or the people around you who say they will take your money and not give you your files
I have enough references to trust you

I do not know you, so there is no point in having bad feelings towards you or doing you harm,
my only aim is to make an income from this business. After your payment,
I will connect to your server as soon as possible to restore your data.

I will also explain how to secure your system after this process so that such incidents will never happen to you again.

Personal Key

e-mail 1 : sunucuverikurtarma@gmail[.]com

Backup

e-mail : serverdatakurtarma@mail[.]ru

QTOX :
A5F2F6058F70CE5953DC475EE6AF1F97FC6D487ABEBAE76915075E3A53525B1D863102EDD50E

Figure 5. Ransom note that contains a TOX ID used by CosmicBeetle, dropped by a LockBit sample. Text was machine translated from Turkish.

Relation to RansomHub

Using leaked builders is a common practice for immature ransomware gangs. It allows them to abuse the brand of their well-established competitors while also providing them with a ransomware sample that usually works properly. The LockBit connection, however, is not the only one we have observed.

In June, we investigated an incident involving ScRansom. From our telemetry, we were able to gather the following:

- On June 3rd, 2024 CosmicBeetle attempted to compromise a manufacturing company in India with ScRansom.

- After failing, CosmicBeetle tried a variety of process-killing tools to remove EDR protection, namely:
  - Reaper,
  - Darkside, and
  - RealBlindingEDR.
- On June 8th, 2024, RansomHub's EDR killer was executed on the same machine.
- On June 10th, 2024, RansomHub was executed on the same machine.

The way RansomHub's EDR killer was executed is very unusual. It was manually extracted via WinRAR from an archive stored at C:\Users\Administrator\Music\1.0.8.zip and executed. Such execution is very unusual for RansomHub affiliates. On the other hand, using the Music folder and manually extracting and executing payloads certainly *is* typical CosmicBeetle behavior.

To our knowledge, there are no public leaks of RansomHub code or its builder (though RansomHub itself is probably based on code bought from Knight, another ransomware gang). Therefore, we believe with medium confidence that CosmicBeetle enrolled itself as a new RansomHub affiliate.

Technical analysis

Similar to the rest of CosmicBeetle's custom arsenal, ScRansom is written in Delphi. The earliest samples we were able to obtain were compiled at the end of March 2023, though, to the best of our knowledge, in-the-wild attacks didn't start before August. ScRansom is under ongoing development.

The GUI is typical for Delphi applications, though not so much for ransomware. All ScRansom samples contain a structured GUI. The older samples, usually named "Static" by the developers, require user interaction to actually encrypt anything. While this may seem a complication, it may be one of the reasons why ScRansom evaded detection for some time, as running such samples in analysis sandboxes does not display any malicious activity.

Launching such an encryptor requires the threat actor to have access to the victim's screen and be able to manipulate their mouse. This is not the first time CosmicBeetle has used this approach – ScHackTool is also a tool that needs to be executed on the victim's machine and requires manual interaction. We are not entirely sure how CosmicBeetle achieves this goal, but guessing from the other tools used, we believe using VPN access with previously stolen credentials and RDP is the most probable scenario.

CosmicBeetle also has experimented with a rarely seen variant named "SSH". The encryptor logic is identical to the other variants, but instead of encrypting local files, it encrypts files over FTP.

Newer builds utilize automation, though only by simulating clicking the correct buttons from code. These automated builds, named "Auto" by the developers, are usually bundled inside an MSI installer together with small tools or scripts to delete shadow copies. The GUI is hidden by default; its most recent version is illustrated in Figure 6.

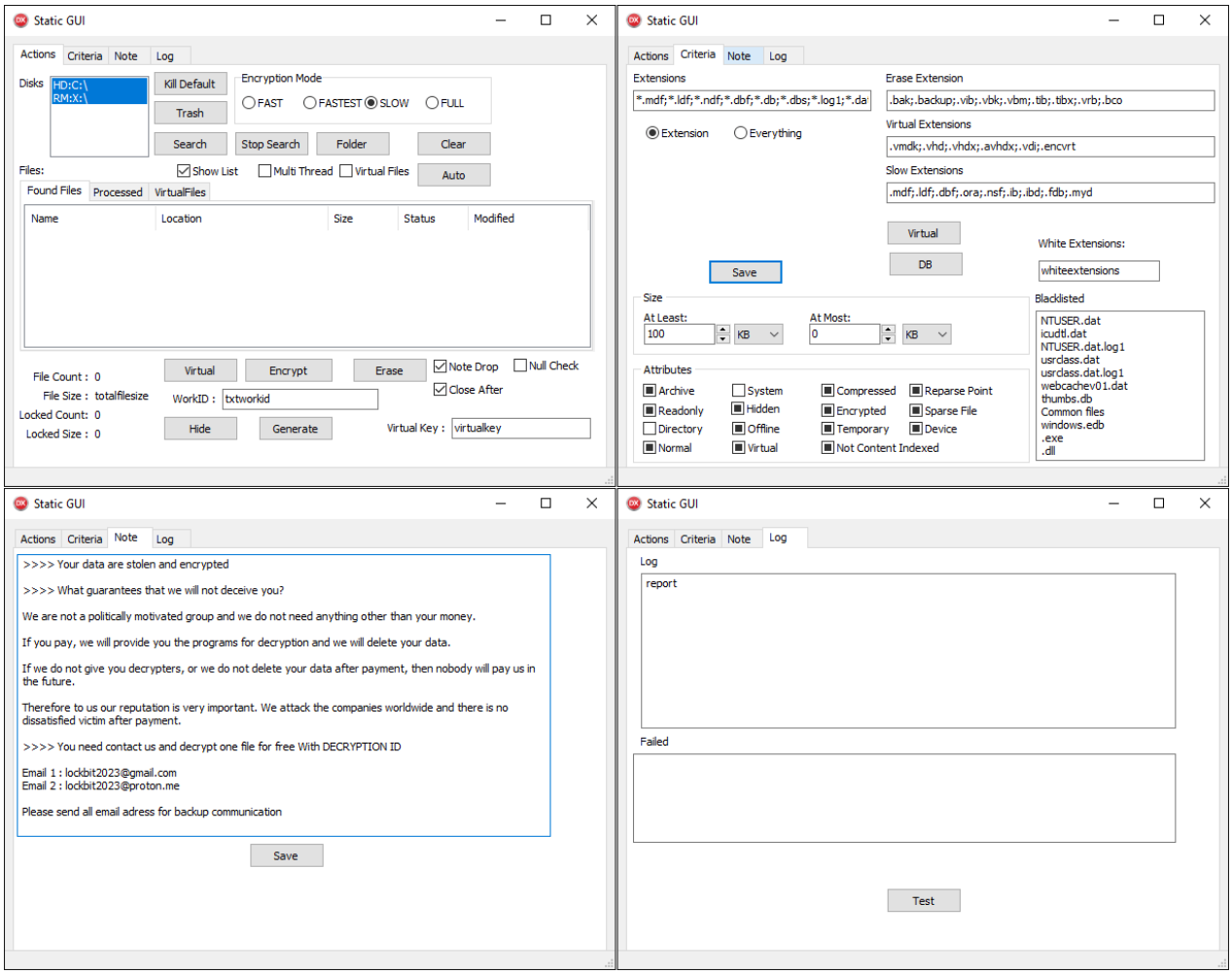

Figure 6. User interface of ScRansom

A complex GUI with a lot of buttons, some of which do nothing, is typical for CosmicBeetle. While the GUI with four tabs looks complex, the functionality is actually very straightforward. ScRansom encrypts files on all fixed, remote, and removable drives based on a hardcoded list of extensions (see *Appendix A: Targeted file extensions*) – this list can be modified via the text box labeled Extensions.

ScRansom employs partial encryption – only parts of the file are encrypted. Five encryption modes are supported:

- FAST
- FASTEST
- SLOW
- FULL
- ERASE

The first four modes simply differ in how the ransomware decides what portions of the file to encrypt. Their utilization seems to still be partially in development, as not all of the modes are used. The last mode, ERASE, is important, however – when applied, selected portions of targeted files are not encrypted but their contents are replaced with a constant value, rendering these files unrecoverable. Which mode is applied for a given file is determined either via the radio buttons in the Actions tab or via the inclusion of its extension in the Criteria tab. The extensions list labeled Virtual Extensions triggers a different encryption function that, however, is identical to the regular one. As you probably guessed, White Extensions should define a list of extensions excluded from encryption, though this feature is not implemented.

Besides encrypting, ScRansom also kills various processes and services (see *Appendix B: Processes killed* and *Appendix C: Services killed*). Recently, a new Delphi sample was split off from ScRansom into a part that we named ScKill, whose sole purpose is to kill processes. ScRansom also employs debug-like features like loading a list of extensions to encrypt from an ext.txt file and ransom note content from a note.txt file.

Encryption

Initial ScRansom samples utilized simple symmetric encryption using AES-CTR-128. Since December 2023, the encryption scheme has been updated. The new scheme is quite (unnecessarily) complex. ScRansom, at the start, generates an AES key we will call ProtectionKey, and an RSA-1024 key pair we will call RunKeyPair.

Every ScRansom sample using this new scheme contains a hardcoded public RSA key from a pair we will call MasterKeyPair. This public key is encrypted using RSA into what CosmicBeetle calls Decryption ID.

For every file, an AES-CTR-128 key that we will call FileKey is generated. Portions of the file are then encrypted using AES with FileKey. When ScRansom finishes encrypting a file, it appends data to its end, specifically:

- The string TIMATOMA (or TIMATOMAFULL if the whole file was encrypted).
- The string TBase64EncodingButton12ClickTESTB64@#$% (TESTB64 in older builds), encrypted by AES using FileKey.
- The following entries, delimited by $ (a dollar sign):
    - Hex-encoded RunKeyPair.Public,
    - Decryption ID,
    - RunKeyPair.Private, encrypted using AES-CTR-128 with ProtectionKey, and
    - FileKey, encrypted using RSA with RunKeyPair.Public.
- Information about encrypted blocks start and their length (absent if the full file is encrypted).

Finally, Decryption ID is stored into a text file named DECRYPTION_IDS.TXT and also written in the ransom note named HOW TO RECOVERY FILES.TXT. Decryption ID *is different each time the encryptor is executed*. On subsequent execution(s), the Decryption IDs are appended to the DECRYPTION_IDS.TXT file, *but not updated in the ransom note*.

The filename (including extension) is then base64 encoded and the .Encrypted extension appended. Despite the complexity of the whole process, we have summarized it in Figure 7.

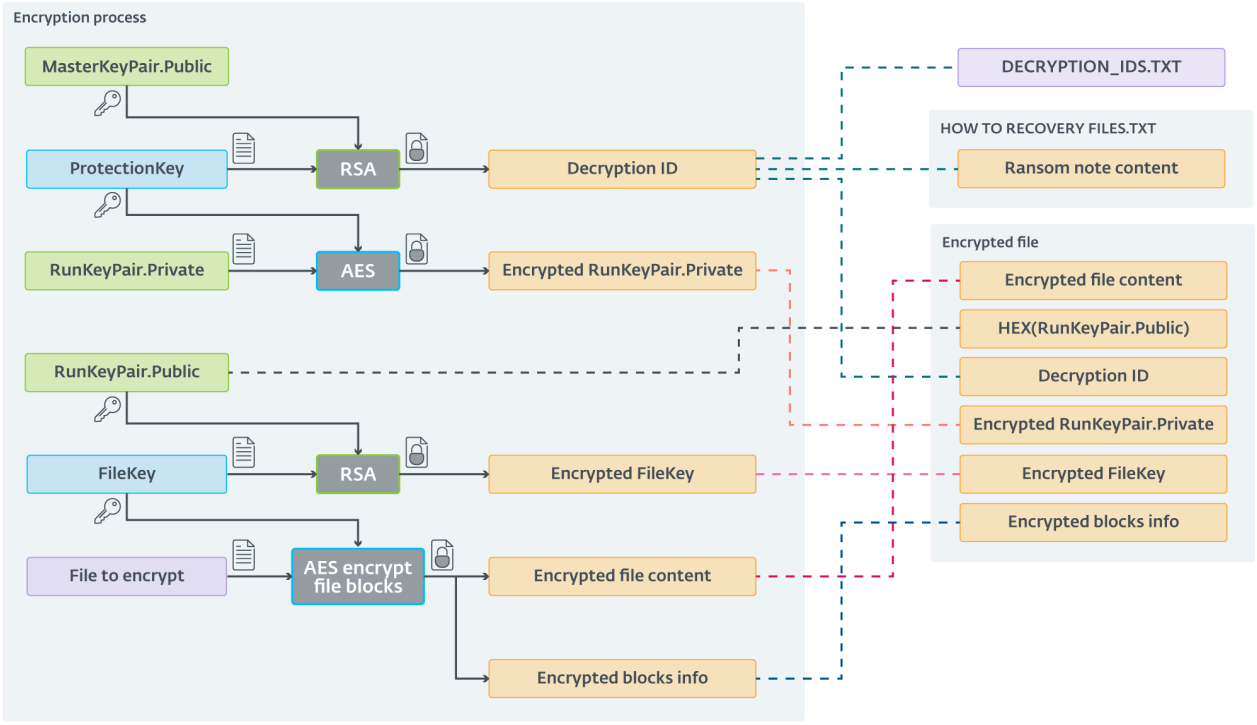

Figure 7. Encryption scheme utilized by the latest ScRansom samples

Decryption

We were able to obtain a decryptor implemented by CosmicBeetle for this recent encryption scheme. CosmicBeetle does not provide its victims with the MasterKeyPair.Private key but with the already decrypted ProtectionKey (that needs to be entered in the field labeled CPriv Aes Key). Additionally, the decryptor expects the Decryption ID, which is useless, as the private key is not provided; indeed, the decryptor ignores its value. The GUI of the decryptor is illustrated in Figure 8.

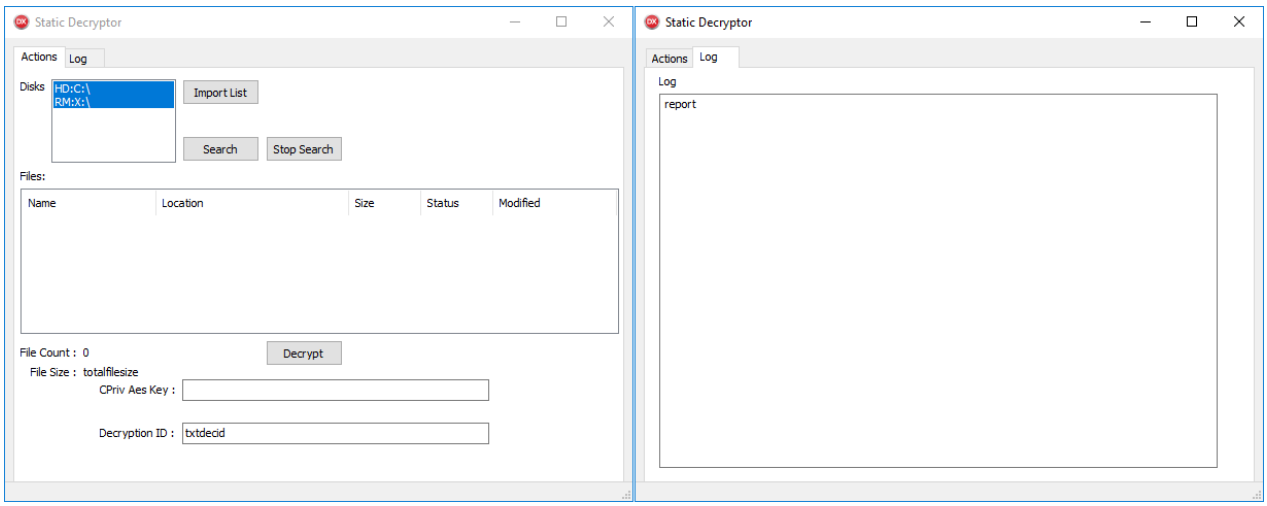

Figure 8. GUI of a ScRansom decryptor. ProtectionKey needs to be entered into the text box labeled CPriv Aes Key

If the correct ProtectionKey is entered, the decryptor works as expected. If victims decide to pay the ransom, they need to collect *all* Decryption IDs from *all* the machines where ScRansom was executed. CosmicBeetle then needs to provide a different ProtectionKey for all of the Decryption IDs. Victims then need to manually run the decryptor on every encrypted machine, enter the correct ProtectionKey (or try all of them), click the Decrypt button and wait for the decryption process to finish.

Moreover, from collaboration with one of the victims, we learned that ScRansom was executed more than once on some machines, leading to even more Decryption IDs. This victim collected 31 different Decryption IDs, requiring 31 ProtectionKeys from CosmicBeetle. Even with those, they were unable to fully recover all of their files. Assuming the encrypted files were not tampered with, this may be the result of missing some Decryption IDs, CosmicBeetle not providing all of the required ProtectionKeys, or ScRansom destroying some files permanently by using the ERASE encryption mode. This decryption approach is typical for an immature ransomware threat actor.

Seasoned gangs prefer to have their decryption process as easy as possible to increase the chances of correct decryption, which boosts their reputation and increases the likelihood that victims will pay. Typically (like in the case of the leaked LockBit Black builder), a decryptor is built together with an encryptor. When distributed to the victim, no additional user effort is required, as the key is already contained in the binary. Additionally, one key is sufficient to decrypt all encrypted files, regardless of where they are in the victim's network.

Conclusion

In this blogpost, we have analyzed CosmicBeetle's activity over the past year. The threat actor is still deploying ransomware, though it switched from Scarab to a new custom family we call ScRansom. Probably due to the obstacles that writing custom ransomware from scratch brings, CosmicBeetle attempted to leech off LockBit's reputation, possibly to mask the issues in the underlying ransomware and in turn to increase the chance that victims will pay.

We also spotted CosmicBeetle trying to deploy LockBit samples built using the leaked builder, though only briefly, before switching back to ScRansom. The threat actor puts efforts into continual development of ScRansom, changing encryption logic and adding features.

Recently, we observed the deployment of ScRansom and RansomHub payloads on the same machine only a week apart. This execution of RansomHub was very unusual compared to typical RansomHub cases we have seen in ESET telemetry. Since there are no public leaks of RansomHub, this leads us to believe with medium confidence that CosmicBeetle may be a recent affiliate of RansomHub.

ScRansom undergoes ongoing development, which is never a good sign in ransomware. The overcomplexity of the encryption (and decryption) process is prone to errors, making restoration of all files unsure. Successful decryption relies on the decryptor working properly and on CosmicBeetle providing *all* necessary keys, and even in that case, some files may have been destroyed permanently by the threat actor. Even in the best-case scenario, decryption will be long and complicated.

> *For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.*
> *ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.*

IoCs

Files

SHA-1	Filename	Detection	Description

SHA-1	Filename	Detection	Description
4497406D6EE7E2EF561C949AC88BB973BDBD214B	auto.exe	Win32/Filecoder.Spacecolon.A	Auto variant of ScRansom.
3C32031696DB109D5FA1A09AF035038BFE1EBE30	Project1.exe	Win32/Filecoder.Spacecolon.B	Auto variant of ScRansom.
26D9F3B92C10E248B7DD7BE2CB59B87A7A011AF7	New.exe	Win32/Filecoder.Spacecolon.A	Static variant of ScRansom.
1CE78474088C14AFB8495F7ABB22C31B397B57C7	Project1.exe	Win32/Filecoder.Spacecolon.B	Auto encryptor variant of ScRansom, Turkish ransom note.
1B635CB0A4549106D8B4CD4EDAFF384B1E4177F6	Project1.exe	Win32/Filecoder.Spacecolon.A	Static SSH encryptor variant of ScRansom.
DAE100AFC12F3DE211BFF9607DD53E5E377630C5	Project1.exe	Win32/Filecoder.Spacecolon.A	Decryptor variant of ScRansom (oldest).
705280A2DCC311B75AF1619B4BA29E3622ED53B6	Rarlab_sib.msi	Win32/Filecoder.Spacecolon.A	MSI file with embedded ScRansom, ScKill, BAT script to stop services, and BAT script to delete shadow copies.

Network

IP	Domain	Hosting provider	First seen	Details
66.29.141[.]245	www.lockbitblog[.]info	Namecheap, Inc.	2023-11-04	Fake LockBit leak site.

Ransom note fragments

Email addresses

- decservice@ukr[.]net
- nonamehack2024@gmail[.]com
- tufhackteam@gmail[.]com
- nonamehack2023@gmail[.]com
- nonamehack2023@tutanota[.]com
- lockbit2023@proton[.]me
- serverrecoveryhelp@gmail[.]com
- recoverydatalife@gmail[.]com
- recoverydatalife@mail[.]ru

Tox IDs

- 91E3BA8FACDA7D4A0738ADE67846CDB58A7E32575531BCA0348EA73F6191882910B72613F8C4
- A5F2F6058F70CE5953DC475EE6AF1F97FC6D487ABEBAE76915075E3A53525B1D863102EDD50E
- F1D0F45DBC3F4CA784D5D0D0DD8ADCD31AB5645BE00293FE6302CD0381F6527AC647A61CB08D
- 0C9B448D9F5FBABE701131153411A1EA28F3701153F59760E01EC303334C35630E62D2CCDCE3

Tor links

- http://nonamef5njcxkghbjequlibwe5d3t3li5tmyqdyarnrsryopvku76wqd[.]onion
- http://noname2j6zkgnt7ftxsjju5tfd3s45s4i3egq5bqtl72kgum4ldc6qyd[.]onion
- http://7tkffbh3qiumpfjfq77plcorjmfohmbj6nwq5je6herbpya6kmgoafid[.]onion

MITRE ATT&CK techniques

This table was built using version 15 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Reconnaissance	T1595.002	Active Scanning: Vulnerability Scanning	CosmicBeetle scans its targets for a list of vulnerabilities it can exploit.
	T1590.005	Gather Victim Network Information: IP Addresses	CosmicBeetle scans the internet for IP addresses vulnerable to the vulnerabilities it can exploit.
Resource Development	T1583.001	Acquire Infrastructure: Domains	CosmicBeetle registered its own leak site domain.
	T1587.001	Develop Capabilities: Malware	CosmicBeetle develops its custom toolset, Spacecolon.
	T1588.002	Obtain Capabilities: Tool	CosmicBeetle utilizes a large variety of third-party tools and scripts.
	T1588.005	Obtain Capabilities: Exploits	CosmicBeetle utilizes publicly available PoCs for known exploits.
	T1588.001	Obtain Capabilities: Malware	CosmicBeetle probably obtained ransomware from RansomHub and the leaked LockBit 3.0 builder.
Initial Access	T1190	Exploit Public-Facing Application	CosmicBeetle gains initial access by exploiting vulnerabilities in FortiOS SSL-VPNand other public-facing applications.
Execution	T1204	User Execution	CosmicBeetle relies on user execution for some of its tools, though this is usually done by the threat actor via RDP.
	T1059.003	Command and Scripting Interpreter: Windows Command Shell	CosmicBeetle executes various BAT scripts and commands.
	T1059.001	Command and Scripting Interpreter: PowerShell	CosmicBeetle executes various PowerShell scripts and commands.
Persistence	T1136.001	Create Account: Local Account	CosmicBeetle often creates an attacker-controlled administrator account.
Defense Evasion	T1078	Valid Accounts	CosmicBeetle abuses valid accounts whose credentials it successfully obtains.

Tactic	ID	Name	Description
	T1140	Deobfuscate/Decode Files or Information	ScRansom samples protect public RSA keys by encryption.
Credential Access	T1110.001	Brute Force: Password Guessing	CosmicBeetle utilizes RDP and SMB brute-force attacks.
	T1212	Exploitation for Credential Access	CosmicBeetle exploits known vulnerabilities to obtain credentials.
Impact	T1485	Data Destruction	CosmicBeetle renders some encrypted files unrecoverable.
	T1486	Data Encrypted for Impact	CosmicBeetle encrypts sensitive files on compromised machines.

Appendix A: Targeted file extensions

This configuration is hardcoded in every ScRansom sample and is subject to frequent change. The following sections contain the most recent configuration at the time of writing.

Filename masks to encrypt

*._ms	*.bkup	*.fp5	*.oeb	*.SLDPRT
*.0001	*.blend	*.fp7	*.ol2	*.sldprt
*.001	*.box	*.frm	*.old	*.sldrpt
*.002	*.bpf	*.ful	*.one	*.slp
*.003	*.btr	*.full	*.ora	*.sna
*.004	*.bup	*.fxl	*.ost	*.sna
*.005	*.c1	*.gan	*.ostx	*.spf
*.006	*.cbd	*.gbk	*.ova	*.spl
*.007	*.cbu	*.gdb	*.pak	*.sql
*.008	*.cdr	*.gho	*.par	*.sqlaudit
.1	*.cdx	*.ghs	*.pbd	*.sqlite
.2	*.cfgbak	*.hbp	*.pcb	*.sqlite3
.3	*.cgd	*.hlp	*.pdb	*.srd
*.3dm	*.couch	*.hrl	*.pdf	*.step
*.3dmbak	*.csv	*.ib	*.pod	*.stm
*.3ds	*.ctf	*.ibd	*.ppt	*.stp
.4	*.d0	*.idx	*.pptx	*.tar
.5	*.d1	*.imd	*.pqb	*.tar.gz
.6	*.d2	*.indd	*.pri	*.tga
.7	*.d3	*.itdb	*.prt	*.tgz
*.7z	*.d4	*.iv2i	*.psd	*.tib
.8	*.da1	*.jet	*.psm	*.tibx
.9	*.da2	*.jpg	*.pst	*.tif
*.a01	*.da3	*.L5X	*.pstx	*.tiff
*.a02	*.da4	*.lbl	*.ptb	*.tmp
*.a03	*.danger	*.ldb	*.qba	*.trc
*.a06	*.dat	*.ldf	*.qbb	*.trn
*.accdb	*.db	*.llp	*.qbm	*.tuf
*.ACD	*.db1	*.log	*.qbw	*.upd
*.adm	*.db2	*.log1	*.qic	*.usr
*.afi	*.dbc	*.lst	*.qrp	*.vbk
*.ai	*.dbdmp	*.mat	*.qsm	*.vbm
*.alt	*.dbf	*.max	*.qvx	*.vct
*.arc	*.dbs	*.mdb	*.rar	*.vcx
*.arc	*.dbw	*.mdbx	*.raw	*.vhd
*.archive	*.df	*.mdf	*.rbf	*.vhdx
*.ard	*.dft	*.mmo	*.rct	*.vib
*.asm	*.diff	*.mov	*.rdb	*.vix
*.avhdx	*.dmp	*.mp4	*.redo	*.vmdk
*.avi	*.doc	*.mrimg	*.rfs	*.vmsd
*.axf	*.docx	*.msg	*.rman	*.vmsn
*.b1	*.dwg	*.mtx	*.rpd	*.vmx
*.bac	*.dxf	*.myd	*.rpo	*.vmxf
*.backup	*.dxt5_2d	*.myi	*.rpt	*.vob
*.bak	*.ebk	*.nb7	*.rtf	*.vrb
*.BBCK	*.edb	*.nbf	*.sai	*.vswp
*.BBCK3	*.edp	*.ndf	*.saj	*.wim
*.bck	*.elg	*.ndk	*.seq	*.wt
*.bco	*.eml	*.ndx	*.sev	*.xls
*.bdmp	*.encvrt	*.nsf	*.sic	*.xlsm
*.bi4	*.fbf	*.nsg	*.sko	*.xlsx
*.bik	*.fbk	*.ntf	*.skp	*.zip
*.bin	*.fbw	*.nx1	*.SLDASM	*ibdata
*.bkf	*.fdb	*.nyf	*.SLDDRW	
*.bkp	*.fmp12	*.obk	*.SLDLFP	

Extensions to encrypt using SLOW mode

.dbf .fdb	.ib .ibd	.ldf .mdf	.myd .nsf	.ora

Extensions targeted for permanent deletion

.backup .bak	.tib .tibx	.vbk .vbm	.vib

"Blacklisted" filenames and path fragments

.bat .cab .cmd .com .dll .drv .encrypted .encrypting .encrypting.map .exe .inf	.ini .msi .nt .ntfs .ocx .reg .sys \Common Files\ \Windows\ c:\windows Common files	icudtl.dat mpenginedb.db NTUSER.dat NTUSER.dat.log1 settings.dat thumbs.db unins0 usrclass.dat usrclass.dat.log1 webcachev01.dat windows.edb

Appendix B: Processes killed

The list below contains two filenames that stand out – Project1.exe, which refers to many ScRansom variants, and app.exe, which is the filename used for older ScHackTool builds.

amService.exe	RuntimeBroker.exe
app.exe	SearchUI.exe
blnsvr.exe	services.exe
cissesrv.exe	ShellExperienceHost.exe
cmd.exe	sihost.exe
CompatTelRunner.exe	smss.exe
conhost.exe	snmp.exe
cqmghost.exe	spoolsv.exe
cqmgserv.exe	SppExtComObj.Exe
cqmgstor.exe	sppsvc.exe
csrss.exe	ssh.exe
ctfmon.exe	sshfs.exe
dwm.exe	sshfs-win.exe
explorer.exe	StartMenuExperienceHost.exe
FCDBLog.exe	svchost.exe
fontdrvhost.exe	taskhost.exe
fsptool-x64.exe	taskhostw.exe
launcher-x64.exe	tasklist.exe
LogonUI.exe	userinit.exe
LsaIso.exe	VGAuthService.exe
lsass.exe	vmtoolsd.exe
lsm.exe	vmware-usbarbitrator64.exe
mobsync.exe	VSSVC.exe
msdtc.exe	wininit.exe
msiexec.exe	winlogon.exe
MsMpEng.exe	wlms.exe
Project1.exe	WmiPrvSE.exe
rdpclip.exe	WUDFHost.exe

Appendix C: Services killed

adws	ntlmssp
aelookupsvc	ntmssvc
ajrouter	onesyncsvc
alg	pcasvc
apphostsvc	pimindexmaintenancesvc
appinfo	plugplay
appmgmt	policyagent
appreadiness	power
appxsvc	profsvc
audioendpointbuilder	protectedstorage
audiosrv	rasman
avpsus.kes	remoteregistry
bdesvc	rmsvc
bfe	rpceptmapper
bits	rpcss
bluetoothuserservice	samss
brokerinfrastructure	scdeviceenum
browser	schedule
bthavctpsvc	sdd_service
camsvc	seclogon
cbdhsvc	securityhealthservice
ccmexec	semgrsvc
cdpsvc	sens
cdpusersvc	sessionenv
certpropsvc	sgrmbroker
cfvspm	shellhwdetection
cissesrv	simptcp

clicktorunsvc
clipsvc
clussvc
comsysapp
coremessagingregistrar
cpqrcmc
cpqvcagent
cryptsvc
dcomlaunch
dcpsvc
deviceassociationservice
deviceinstall
dfs
dfsr
dhcp
diagtrack
dispbrokerdesktopsvc
displayenhancementservice
dmserver
dns
dnscache
dosvc
dps
dssvc
dtsapo4service
dusmsvc
efs
ersvc
eventlog
eventsystem
fa_scheduler
fdphost
fontcache
ftpsvc
gisvc
gpsvc
helpsvc
hidserv
httpfilter
ias
iisadmin
ikeext
installservice
intel(r) proset monitoring service
iphlpsvc
ismserv
kdc
keyiso
klnagent
lanmanserver
lanmanworkstation
lfsvc
licensemanager
lmhosts
lsm
mpssvc
msdtc
msiscsi
msmframework
ncbservice
spooler
ssdpsrv
sstpsvc
staterepository
storsvc
swprv
sysdown
sysmain
sysmgmthp
systemeventsbroker
tabletinputservice
tapisrv
termservice
themes
tiledatamodelsvc
timebrokersvc
tokenbroker
trkwks
trustedinstaller
ualsvc
umrdpservice
unistoresvc
userdatasvc
usermanager
ususosvc
uxsms
vaultsvc
vds
vflragentd
vgauthservice
vm3dservice
vmauthdservice
vmicheartbeat
vmickvpexchange
vmicrdv
vmicshutdown
vmictimesync
vmicvss
vmtools
vmusbarbservice
vmware-converter-agent
vss
w32time
w3svc
was
wbiosrvc
wcmsvc
wcncsvc
wdiservicehost
wdisystemhost
wdnissvc
windefend
WinFsp
winfsp.launcher
WinFsp.Launcher
winhttpautoproxysvc
winmgmt
winrm
wins
wlansvc

netlogon	wlidsvc
netman	wlms
netprofm	wpnservice
netsetupsvc	wpnuserservice
nfsclnt	wscsvc
nfsservice	wsearch
nla	wuauserv
nlasvc	wudfsvc
nsi	wzcsvc
ntds	zabbix agent

Let us keep you up to date

Sign up for our newsletters