

Resecurity | Ransomware Attacks against the Energy Sector on the Rise - Nuclear and Oil & Gas are Major Targets in 2024

Oil, Gas, Energy, Ransomware, Nuclear Energy, Cyber Threats, Cyber Attacks



Resecurity has identified an alarming rise in ransomware operators targeting the energy sector, including nuclear facilities and related research entities. Over the last year, ransomware attackers have targeted energy installations in North America, Asia, and the European Union. In the EU, *Handelsblatt* reported that ransomware attacks targeting the energy sector more than doubled in 2022 over the previous year, with defenders recording 21 attacks through the past October.

After a brief, sectoral ‘cease-fire’ following the 2021 Colonial Pipeline ransomware attack, cybercriminals are once again homing in on energy-industry targets. Threat actors reason that the seizure of the higher-value Critical Infrastructure (CI) assets handled by these firms will yield more lucrative payouts in ransom negotiations. Factors that make energy firms more vulnerable to ransomware attacks include complexities in converging IT and operational technology (OT) networks, third-party risks, and historic geopolitical fragmentation.

Backdropped by the conflicts in Ukraine and Gaza, Resecurity has also observed suspected cases of state-sponsored espionage activity masquerading as financially motivated ransomware attacks. While Israeli entities have not yet reported any meaningful ransomware attacks, the eruption of war in Gaza in October has fomented a concurrent rise in threat actor **activity** targeting Israeli energy installations. This activity includes propaganda-oriented hacktivist campaigns and more serious threat actors like Storm-1133, a group initially flagged by Microsoft threat researchers.

Resecurity’s research delves deeper into unique ransomware trends cited by the Department of Homeland Security in their recently [published](#) Intelligence Enterprise Homeland Threat Assessment. “Between January 2020 and December 2022, the number of known ransomware attacks in the United States increased by 47 percent,” according to the DHS report. The agency also noted that “ransomware attackers extorted at least

\$449.1 million globally during the first half of 2023 and are expected to have their second most profitable year.”

In the wake of the MOVEit Transfer supply-chain extortion [campaign](#), which has claimed over 2,180 victims so far, 2023 may be the most profitable year ever for ransomware actors. According to the DHS report, the broader trend driving the ransomware industry’s increasing ROI is the return of “big game hunting,” or targeting large organizations. The emerging tactics being deployed by ransomware actors in their big-game extortion ‘safaris’ include intermittent encryption, more modern specialized programming languages, and dual ransomware attacks involving more than one variant.

According to the FBI, these dual-variant campaigns typically sequence their attacks over 48 hours. As CIOp demonstrated in their MOVEit campaign, there is also rising concern that attackers may be eschewing the in-house development of encryption lockers altogether in favor of more efficient data theft schemes. By quickly seizing and exfiltrating data, ransomware actors can pivot into the extortion phase of the attack cycle more immediately. According to the DHS report, intermittent encryption enables threat actors to “encrypt systems faster and reduce the chances of being detected,” regarding the first two emerging ransomware tactics cited.

The enhanced efficiency and evasiveness offered by the above technique are selling points that can help cyber-extortion gangs “entice affiliates to join their Ransomware-as-a-Service operations,” noted the DHS report. The report also said that next-generation programming languages like Rust and Golang, for example, can enhance threat actors’ abilities to “adapt and individualize their attacks.”

Overall, the energy sector was the fourth-most-[targeted](#) sector last year, accounting for 10.7% of all cyberattacks. The DHS report warned that “state and non-state cyber actors continue to seek opportunistic access to critical infrastructure sector targets for disruptive and destructive attacks.” Additionally, “malicious cyber activity targeting the United States has increased since the beginning of the Russia-Ukraine conflict,” noted the DHS report.

With no clear end to the Israeli-Hamas and Russo-Ukrainian conflicts in sight, Ransomware attacks targeting energy firms are becoming increasingly prevalent in the U.S. and globally. The following white paper will provide a timeline of all significant energy-sector ransomware attacks over the last year, present HUNTER (HUMINT) research on Dark Web solicitations for energy-sector access, and detail findings from our undercover ransom negotiations with threat actor Black Basta.

Key Takeaways

- Resecurity has identified several Initial Access Brokers (IABs) operating on the Dark Web actively seeking credentials and other unauthorized intrusion methods for the energy sector. Some of these IABs are even promoting unauthorized access to nuclear energy firms. Furthermore, Resecurity has identified numerous posts on major cybercriminal forums, including RAMP (the Russian Anonymous Market Place), where threat actors have profited and continue to profit from illegal network access.
- Per Resecurity investigations, ransomware attacks on the energy sector have significantly increased. Malicious campaigns have been observed in North America, Asia, and the European Union (EU). Cybercriminals target this sector, assuming they can command more lucrative ransom payments due to the higher-value data assets involved. These attacks prove that critical infrastructure (CI) data assets are more valuable to ransomware groups than those stored by other economic sectors.
- Resecurity anticipates that criminal entities operating on the Dark Web and professional ransomware gangs will intensify their targeting of the energy industry. These attackers will co-opt independent actors and IABs to help them profit from illicit network intrusions.
- Ransomware operators targeting energy firms will continue to increase their extortion demands beyond \$7 million, weaponizing their essentiality to CI operations. One aggravating factor that can justify

payouts of this size to victim organizations is the potential for the devastating disruption of industrial processes within their surrounding environment.

- Nuclear energy organizations are high-priority targets for ransomware operators and advanced threat groups seeking to participate in cyber espionage. Leaked data from these entities may serve as a smokescreen for more intricate attacks planned before any public announcement of these incidents. This tradecraft can make it more challenging for breach investigators to determine the true motives behind a cyberattack.
- Governments and private-sector stakeholders are increasingly concerned about the rise in ransomware attacks targeting the energy sector. This disturbing trend destabilizes geopolitical relations, capital markets, public safety, and national security.

Analysis of Ransomware Attacks Targeting the Energy Sector (2022-2023)

After analyzing ransomware incidents that impacted the energy sector over the past year, Resecurity has found that extortion demands can vary from tens of thousands to millions of dollars. In the following chart, we have detailed several high-profile attacks on energy firms, with attributions to their corresponding perpetrators.

Date (newest to oldest)	Ransomware Group	Victim Company
February 2023	Medusa	PetroChina
February 2023	LockBit 3.0	Phihong
February 2023	Black_Basta	ACEA
December 2022	Black-Cat / ALPHV	Empresas Públicas de Medellín (EPM)
October 2022	Hive	Tata Power Company Limited
September 2022	N/A	Electricity Company of Ghana (ECG)
September 2022	LockBit 3.0	Canadian Solar
August 2022	BlackCat / ALPHV	Gestore dei Servizi Energetici GSE S.p.A.
August 2022	BlackCat/ALPHV (suspected)	Eni S.p.A.
August 2022	Ragnar Locker	DESFA
August 2022	BlogXX	Oil India Limited
April 2022	Hive	STELCO
March 2022	Hive	Romp petrol
March 2022	BlackCat/ALPHV (Suspected)	SEA-Tank
February 2022	BlackCat Ransomware (Suspected)	Oiltanking, SEA - Invest and Evos



In the context of the Ukraine war, the most geopolitically noteworthy attacks include the steady stream of intrusions by actors like BlackCat/ALPHV, Qilin, and Black Basta targeting energy installations and refining hubs in the Low Countries, Switzerland, Italy, and Germany. Once the engine of the European economy, Germany has been particularly hard hit by the transition away from Russian natural gas imports resulting from war-related sanctions.

As such, Germany's energy infrastructure has been especially vulnerable. In this regard, ALPHV's coordinated attacks on Oiltanking in Germany, Invest-SEA in Belgium, Evos in the Netherlands, and the Amsterdam-Rotterdam-Antwerp oil terminals in February 2022 are particularly noteworthy. These attacks all immediately coincided with the Russian invasion of Ukraine.

ALPHV, a trailblazer in modern-language-coded ransomware, is considered a Russian-nexus threat group. In the context of Germany, Quilin's attack on Thornburi Energy Storage Systems (TESM), a Bangkok-based plug-in battery manufacturer, is also significant. Despite being a Thai firm, TESM is a key partner of German auto manufacturer Mercedes-Benz AG, with the latter recently investing €100 million in the battery maker.

As for other energy-related attacks in the EU, ALPHV's and Black Basta's attacks on Italian public utilities like Acea, the country's national energy agency, Gestore dei Servizi Energetici S.p.A. (GSE), and multinational oil firm Eni S.p.A. are also significant. These attacks occurred two months before the Italian general election in 2022, which came earlier than scheduled due to the collapse of former Prime Minister Mario Draghi's government.

A widely contentious issue leading up to the eventual election of current Prime Minister Giorgia Meloni was support for the Ukrainian struggle against Russia. Apart from ransomware attacks, CIOp's Memorial Day supply-chain attack campaign compromised at least 2,180 victims, including British multinational oil firm Shell plc, German industrial heating pump manufacturer Siemens AG, French energy company Schneider Electric, and the U.S. Department of Energy.

Another interesting development noted by HUNTER analysts is the uptick in attacks targeting the Indonesian energy sector this year. This trend is noteworthy, given that the country's presidential election is scheduled for 2024. Russian nexus groups like Medusa and ALPHV have claimed credit for attacks targeting Indonesian energy firms.

One last development HUNTER analysts noted was the growing alliance between hacktivist groups and ransomware operators, specifically the recently announced alliance between GhostSec and Stormous, respectively. The GhostSec-Stormous alliance has vowed to prioritize attacks on U.S., Ukrainian, Indian, Peruvian, and Vietnamese targets. In July, the duo announced the compromise of the Cuban Ministry of Energy and Mines data. Nuclear Energy Firms Are Becoming Priority Targets

Backdropped by the Russo-Ukrainian conflict, threat actor interest in nuclear energy firms and related entities has increased. This past January, *Reuters* reported that a Russian advanced persistent threat (APT) group dubbed 'Cold River' by researchers "targeted three nuclear research laboratories in the United States" in the Summer of 2022. This malicious campaign occurred between August and September of last year.

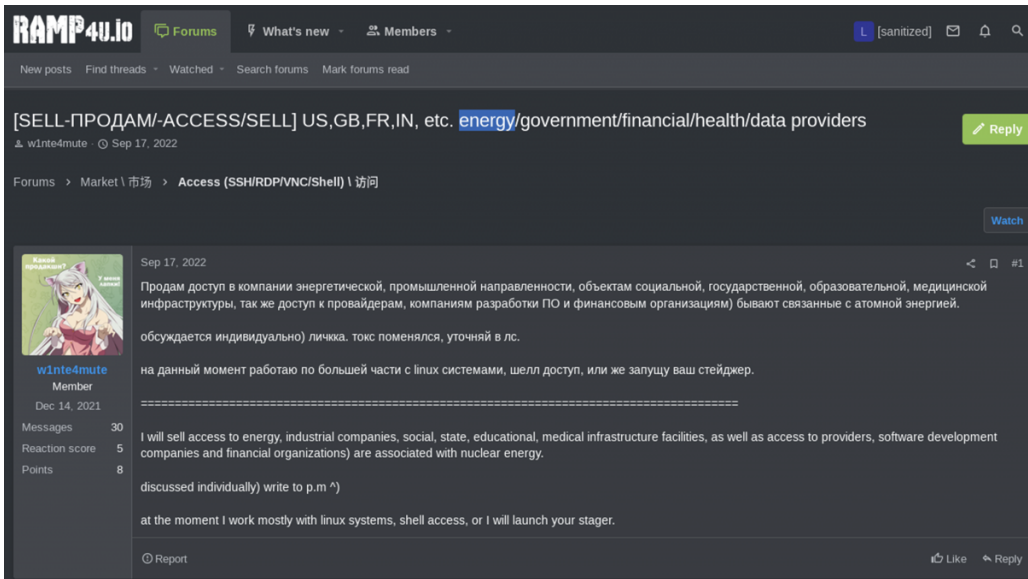
"Cold River targeted the Brookhaven (BNL), Argonne (ANL), and Lawrence Livermore National Laboratories (LLNL), according to internet records that showed the hackers creating fake login pages for each institution and emailing nuclear scientists in a bid to make them reveal their passwords," reported *Reuters*.

In this threat environment, Resecurity has noticed growing interest from threat actors soliciting access to nuclear-sector entities. The following images are screenshots of posts Resecurity investigators captured from various cybercrime forums. Specifically, HUNTER analysts mined threat intelligence from RAMP, XSS, Exploit, Breach Forums, and Telegram channels.

Regarding publicly accessible nuclear access listings, Breach Forums is the most fertile hub for open-source intelligence. The images below depict examples of Initial Access Brokers (IABs) offering access to nuclear energy-sector corporate networks. This first screencap is from the RAMP forum.

RAMP

In the Ramp post from December 2021 below, threat actor ‘W1nte4mute’ solicits access to energy provider networks, including those that “are associated with nuclear energy.”



RAMP4U.io Forums What's new Members [sanitized]

New posts Find threads Watched Search forums Mark forums read

[SELL-ПРОДАМ/-ACCESS/SELL] US,GB,FR,IN, etc. [energy/government/financial/health/data providers](#) Reply

w1nte4mute Sep 17, 2022

Forums > Market \ 市场 > Access (SSH/RDP/VNC/Shell) \ 访问 Watch

Sep 17, 2022

Продам доступ в компании энергетической, промышленной направленности, объектам социальной, государственной, образовательной, медицинской инфраструктуры, так же доступ к провайдерам, компаниям разработки ПО и финансовым организациям) бывают связанные с атомной энергией.

обсуждается индивидуально) личка, токс поменялся, уточняй в лс.

на данный момент работаю по большей части с linux системами, шелл доступ, или же запущу ваш стейджер.

I will sell access to energy, industrial companies, social, state, educational, medical infrastructure facilities, as well as access to providers, software development companies and financial organizations) are associated with nuclear energy.

discussed individually) write to p.m ^)

at the moment I work mostly with linux systems, shell access, or I will launch your stager.

Report Like Reply

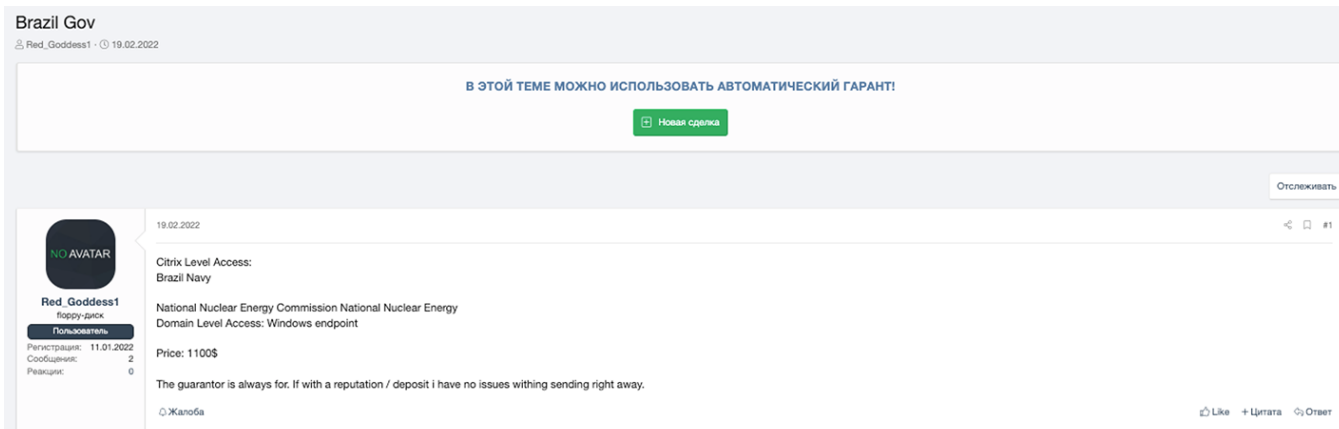
w1nte4mute Member Dec 14, 2021 Messages: 30 Reaction score: 5 Points: 8

Threat actor ‘W1nte4mute’ solicits access to energy provider networks, source: RAMP.

Resecurity analysts identified similar offerings on the XSS and Exploit cybercriminal forums.

XSS/Exploit

In the below XSS and Exploit forum posts from February last year, a threat actor, Resecurity, presumed to be the same individual, solicits domain-level access to Brazil’s “National Nuclear Energy Commission National Nuclear Energy” for \$1,100. The threat actor selling this access on XSS uses the handle ‘Red_Goddess1.’



Brazil Gov

Red_Goddess1 19.02.2022

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧЕСКИЙ ГАРАНТ!

Новая сделка

Отслеживать

19.02.2022

Citrix Level Access:
Brazil Navy

National Nuclear Energy Commission National Nuclear Energy
Domain Level Access: Windows endpoint

Price: 1100\$

The guarantor is always for. If with a reputation / deposit I have no issues withing sending right away.

Like + Цитата Ответ

Red_Goddess1 Пользователь Регистрация: 11.01.2022 Сообщений: 2 Репутация: 0

‘Red_Goddess1’ solicits access to Brazil’s National Nuclear Energy Commission, source: XSS.is.

Around the same time, a threat actor using the Sandw0rm handle just registered this Exploit. A week after the initial XSS posting, the forum account solicits the same access to Brazil’s NNEC at a starting price of \$500, or less than half of the original asking amount. It’s also worth noting that this threat actor probably has no relation with the real Sandworm (nation-state APT group also known as Voodoo Bear), given the relatively low asking price for this access.



Forums Guidelines Staff Online Users Search

Home > Commerce > Auctions > Brazil-Gov-Military-Energy Commission Unread



S Brazil-Gov-Military-Energy Commission

By Sandw0rm, 9 hours ago in Auctions

Sandw0rm
byte
●

Paid registration
● 0
0 posts
joined
02/27/22 (ID: 126282)
Activity
хакинг / hacking

Posted 9 hours ago

1. Access Type: Citrix:
Brazil-Gov -Navy
2. Brazil- Nuclear Energy Commission
Network Access to Endpoint
Domain Only
AV: Symantec Endpoint

Start: 500\$
Step: 50\$
Blitz: 2,000\$

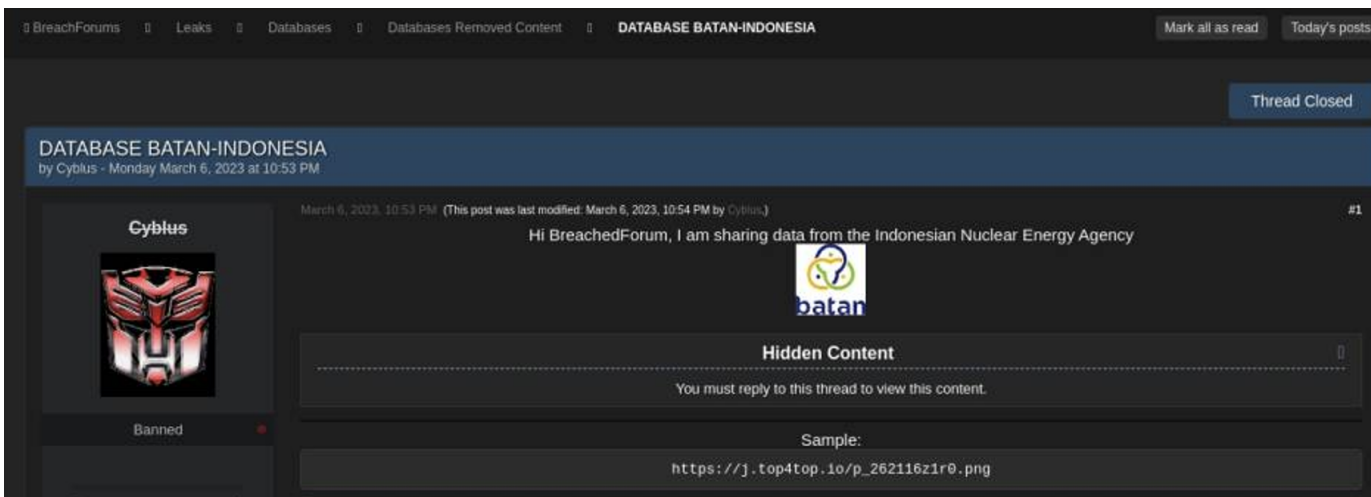
Threat actor 'Sandw0rm' solicits the same access to Brazil's NNEC, source: Exploit.in.

Breach Forums

In the below Breach Forums post from August 12, 2023, threat actor 'WAIL_CRINAL' solicits access to a database belonging to Israel's Neve Ne'em nuclear reactor for the relatively low price of \$900. 'WAIL CRINAL' claims that this dataset includes full names with all information about Officials and professors with their residence addresses; 10 GB of confidential documents, including components and materials used in experiments; dimensions, levels, and locations of the reactors; emails and IPs and passwords for login (SSH SMTP servers).

Indonesia's National Nuclear Energy Agency (Batan)

In March 2023, threat actors leaked data 1.4 GB of data stolen from the **National Nuclear Energy Agency of Indonesia (Batan)** on Breach Forums. The motive behind this attack may have been hacktivism to protest the Indonesian government and law enforcement during widespread unrest over fuel prices.



Threat actor 'Cyblus' leaks Batan data, source: Breach Forums.

Some advanced cyber-espionage groups intentionally disguise their actions to appear like typical cyber criminals or hacktivists. The 1.4 GB of Batan data was recently re-published on the "A.I.G." Telegram channel, short for the Atlas Intelligence Group, AKA the Atlantis Cyberarmy. This group offers various illegal services, like distributed denial of service attacks (DDoS) and access to stolen data.

Atlantis - CyberArmy - A.I.G

1,498 members

Pinned message #65

Which hack should we announce as next ?

Indonesian nuclear agency internal files leak

Details:

These 1.4 gb worth of files regarding the Nuclear power authority in Indonesia are being leaked in response to police brutality and corruption by the Indonesian government.

Download link: [htt](https://drive.google.com/file/d/1buHF7ph7GGXRdbkSLF188yfZoE_MTC)

[ps://drive.google.com/file/d/1buHF7ph7GGXRdbkSLF188yfZoE_MTC/SW/view?usp=sharing](https://drive.google.com/file/d/1buHF7ph7GGXRdbkSLF188yfZoE_MTC/SW/view?usp=sharing)

← 1 7:17 PM

Atlantis CyberArmy solicits access to Batan data initially posted on Breach Forums, source: Telegram.

Nuclear Power Production and Development Company of Iran (AEOI)

Around May 2023, threat actors leaked more than 100,000 emails that were stolen from the Nuclear Power Production and Development Company of Iran (AEOI) on Breach Forums. The AEOI manages the Bushehr Nuclear Power Plant (BNPP) and leads Iranian research into nuclear fuel cycle development. AEOI's research initiatives include uranium exploration, mining, and conversion. Attackers exfiltrated 75GB of sensitive Iranian nuclear data.


BreachForums Leaks Other Leaks DOCUMENTS Releases: Nuclear Power Development Company of Iran (75 GB) Mark all as read Today's posts

New Reply

Releases: Nuclear Power Development Company of Iran (75 GB)

by haxdiver - Friday February 3, 2023 at 10:21 AM

haxdiver



M.V.P User

Posts: 376
Threads: 211
Joined: Sep 2022
Reputation: 316

February 3, 2023, 10:21 AM #1

Nuclear Power Production and Development Company of Iran

Over 100,000 emails from the Nuclear Power Production and Development Company of Iran, which owns the Bushehr Nuclear Power Plant Operation Company and runs Iranian research and development in the nuclear fuel cycle, including uranium exploration, mining and conversion.

The company was linked to Iran's proliferation of nuclear weapons by the European Union in 2007, and by the British and Japanese governments in 2015. It was removed from the E.U. sanctions list in January 2016 as part of the Joint Comprehensive Plan of Action.

This data can be downloaded via MAGNET file size 75GB

```
magnet:?xt=urn:bt1h:b7581a1f66de150b505d602361deb6e49dead8d8&dn=nppd&tr=http%3A%2F%2Ftracker.openbittorrent.com%3A80%2Fannounce&tr=udp%3A%2F%2Ftracker.openbittorrent.com%3A6969%2Fannounce&tr=https%3A%2F%2Fopentracker.i2p.rocks%3A443%2Fannounce&tr=udp%3A%2F%2Fopen.stealth.si%3A80%2Fannounce&tr=udp%3A%2F%2Fexodus.desync.com%3A6969%2Fannounce&tr=udp%3A%2F%2Fexodus.desync.com%3A6969%2Fannounce
```

Quote:

Research

Leaked documents reveal the mail of the nuclear power company in Iran (Akhbar Al Aan)

Iranian hacker group releases details about nuclear program (i24 News)

Iranian hackers claim to have obtained files of Iran's 'dirty nuclear projects' (Jerusalem Post)

Hacktivists say they stole 100,000 emails from Iran's nuclear energy agency (The Register)

Do backup/Download content due to BF all links index in google search my all link down/removed (google drive & mega.nz) within days.
DO NOT LEECH IT PLEASE! 😊

Threat actor leaks 75 GB of data from the AEOL source Breach Forums.

Doosan (South Korea)

One of the first ransomware crews to target the nuclear sector was BlogXX, a sophisticated threat actor group that included former ReEvil members. Doosan, a Fortune 500 South Korean multinational conglomerate, was one notable victim BlogXX touted on their leak site. This company is vital in supporting critical infrastructure in South Korea, including the nuclear energy sector. Doosan is also the corporate parent to Bobcat and Škoda Power. BlogXX claimed to have stolen over 1.6 TB of sensitive data from Doosan and its business partners. The threat actors also published multiple samples of the ransomed files to prove their claims.

Doosan Group Views: 177110

Doosan Group is a South Korean multinational conglomerate. In 2009, the corporation entered the Fortune Global 500 index. It is the parent company of Bobcat and Skoda Power. Doosan Group is the oldest operating company in South Korea and one of the world's top ten heavy equipment manufacturers. It was hacked by a group of hackers REvil. More than 1.6Tb of data (drawings, contracts, etc.) was also downloaded. Information was also downloaded directly from Doosan partners. The main attack fell on Doosan Machine Tools, thanks to which access to the entire Doosan infrastructure was gained. Due to the inattention of the IT department of Doosan MT, all databases, virtual machines and backups were encrypted, which stopped the work of this company

First data pack:
http://ttn4qgpgvvy6tuezezxhwiukmm2t6zzawj6p3w3jprve36f43zxr24qd.onion/DOOSANMT_DNSolutions/

Company Code: 4100 Doosan Machine Tools A
 Financial Statement: D107 IFRS Financial Statement (English)
 Fiscal year: 2021
 Periods: 04
 Currency: USD
 Display: Parts non-divided (B161+B162+B163+B261+B262)

Financial Statement	Text	Total
D107	Assets	165,112,600.14
	I. Current Assets	155,522,128.46
	Cash and Cash Equivalent	20,402,454.67
	Accounts and Notes Receivable	53,892,985.96
	Inventory	78,024,930.18

BlogXX Dark Web leak site, source: BlogXX.

In early December 2020, approximately 1.5 years before BlogXX's ransom announcement, Resecurity notified Doosan and the Korean National Computer Emergency Response Team (KN-CERT) about a potential breach impacting their Active Directory. At the time, our team was tracking an IAB soliciting access to Doosan and promoting a listing of the company's Active Directory. Resecurity analysts acquired exclusive access to this listing, which has never been posted publicly on the BlogXX leak site. See the screenshot below.

Standard	Standard	Standard	Standard	Standard
1 Name	DNSHostName	Enabled	IPv4Address	Operating System
2 CHEINDC01	CHEINDC01.corp.doosan.com	True	10.5.212.11	Windows Server 2008 R2 Standard Service Pack 1 6.1
3 PD013416	PD013416.corp.doosan.com	True	10.23.8.49	Windows 10 Pro 10.0 (15063)
4 PWRN1007	PWRN1007.corp.doosan.com	True	10.29.112.139	Windows 7 Enterprise Service Pack 1 6.1 (7601)
5 v-0900000-20096	v-0900000-20096.corp.doosan.com	True	10.5.90.28	Windows 7 Enterprise K Service Pack 1 6.1 (7601)
6 I0213893N1114	i0213893N1114.corp.doosan.com	True	10.229.195.63	Windows 10 Enterprise 10.0 (17134)
7 TD445	td445.corp.doosan.com	True	10.5.32.67	Windows 10 Enterprise 10.0 (17134)
8 HYOHYUNGAN20010	hyohyungan200102.corp.doosan.com	True	10.115.30.33	Windows 10 Pro 10.0 (18363)
9 PRG-UD-070	PRG-UD-070.corp.doosan.com	True	10.52.105.52	Windows 10 Pro 10.0 (18363)
10 PL011411	PL011411.corp.doosan.com	True	10.5.130.100	Windows 10 Enterprise 10.0 (17134)
11 55PE14831	55PE14831.corp.doosan.com	True	10.30.106.7	Windows 10 Enterprise 10.0 (18363)
12 I0359997	I0359997.corp.doosan.com	True	10.32.60.31	Windows 7 Enterprise K Service Pack 1 6.1 (7601)
13 CHANJUNT0521	chanjunT0521.corp.doosan.com	True	10.116.2.224	Windows 10 Enterprise 10.0 (17134)
14 YEEUNHUHD200102	yeeunhuhD200102.corp.doosan.com	True	10.110.4.239	Windows 10 Enterprise 10.0 (17134)
15 PRG-UD-071	PRG-UD-071.corp.doosan.com	True	10.52.105.67	Windows 10 Pro 10.0 (18363)

Doosan's stolen Active Directory listing, source: BlogXX.

Resecurity assesses that the initial Doosan intrusion likely occurred around 12/3/20 before evolving into a more serious breach. Around the same time, BlogXX also targeted major enterprises, government agencies, and organizations involved in nuclear research, including **The Institute for Nuclear Research Pitesti (ICN)** in Romania. Unlike high-margin private sector firms, research organizations are undesirable for financially motivated cyber-threat actors, as they are less likely to manage significant financial assets.

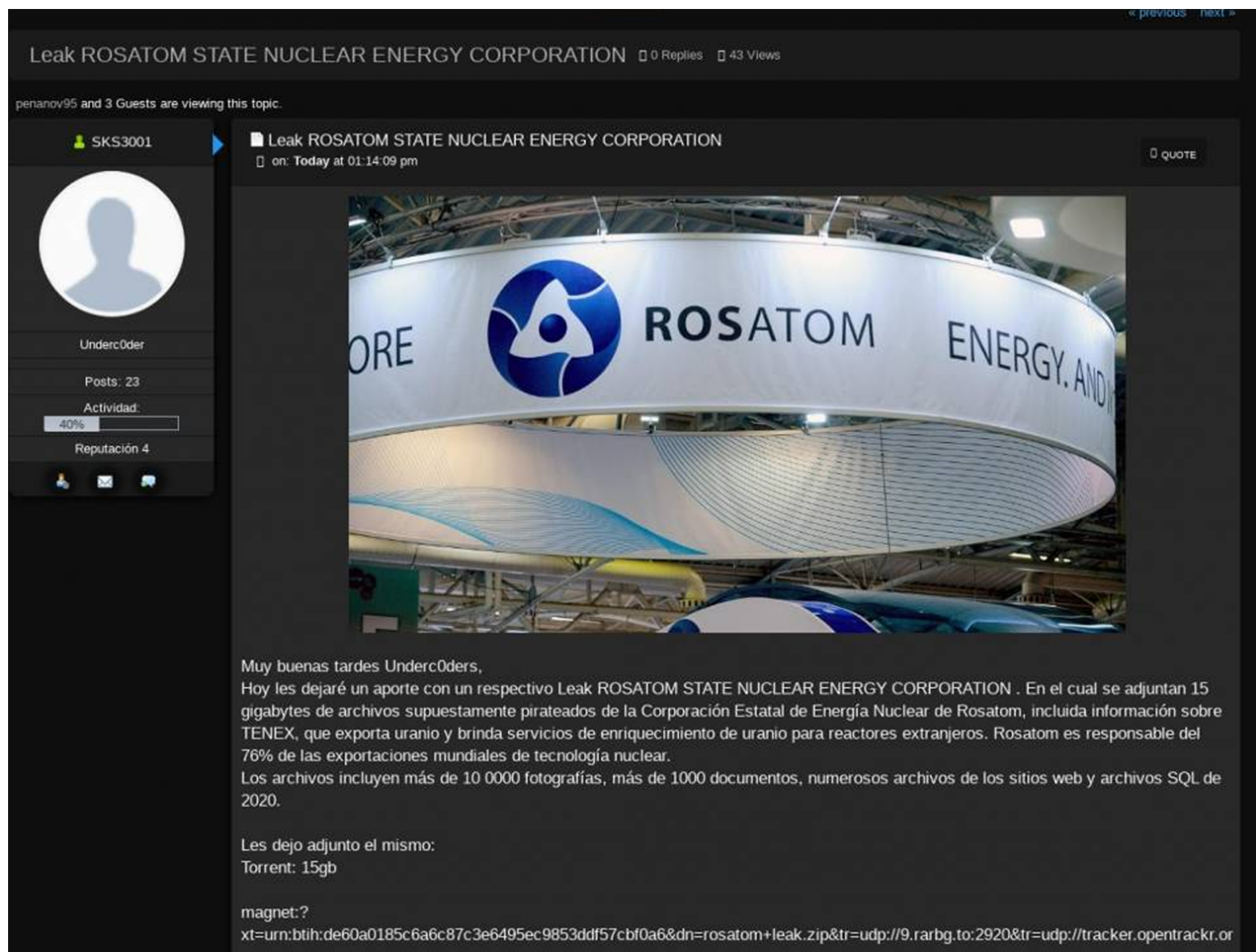
For this reason, the motivation for BlogXX's ransomware attack on the ICN is more likely to be cyber espionage. Resecurity has also notified Romania's National Computer Security Incident Response Team (CERT-RO) and passed information about this activity to competent authorities. While Resecurity assesses

this activity to be independent of REvil/BlogXX, it's possible the ransomware operators engaged directly with the broader syndicate(s).

One potential scenario could be that the actor promoting ICN access was operating either as an IAB or one of the group's affiliates. Another possibility is that the threat actor was conducting reconnaissance for a more powerful attack, which was then disguised as cybercriminal activity. The line between state actors and cybercriminals is often blurred, and these attacks raise concerns about cybersecurity regulation and geopolitical risks.

Geopolitical Contagion

As tensions rise due to Russia's invasion of Ukraine, there has been a dangerous increase in cyberattacks targeting critical infrastructure sectors, including energy. The situation in Ukraine has escalated to a full-blown war zone, and there have been multiple incidents of cyber espionage targeting the nuclear industry. In March 2022, Resecurity assessed that the alleged Russian-state nuclear energy corporation ROSATOM hack was likely retaliatory.




Leak ROSATOM STATE NUCLEAR ENERGY CORPORATION 0 Replies 43 Views

penanov95 and 3 Guests are viewing this topic.

SKS3001 | **Underc0der**

Leak ROSATOM STATE NUCLEAR ENERGY CORPORATION
on: Today at 01:14:09 pm



Muy buenas tardes Underc0ders,
Hoy les dejaré un aporte con un respectivo Leak ROSATOM STATE NUCLEAR ENERGY CORPORATION . En el cual se adjuntan 15 gigabytes de archivos supuestamente pirateados de la Corporación Estatal de Energía Nuclear de Rosatom, incluida información sobre TENEX, que exporta uranio y brinda servicios de enriquecimiento de uranio para reactores extranjeros. Rosatom es responsable del 76% de las exportaciones mundiales de tecnología nuclear.
Los archivos incluyen más de 10 000 fotografías, más de 1000 documentos, numerosos archivos de los sitios web y archivos SQL de 2020.

Les dejo adjunto el mismo:
Torrent: 15gb

magnet:?xt=urn:btih:de60a0185c6a6c87c3e6495ec9853ddf57cbf0a6&dn=rosatom+leak.zip&tr=udp://9.rarbg.to:2920&tr=udp://tracker.opentrackr.or

Threat actor 'Underc0der' leaks ROSATOM data

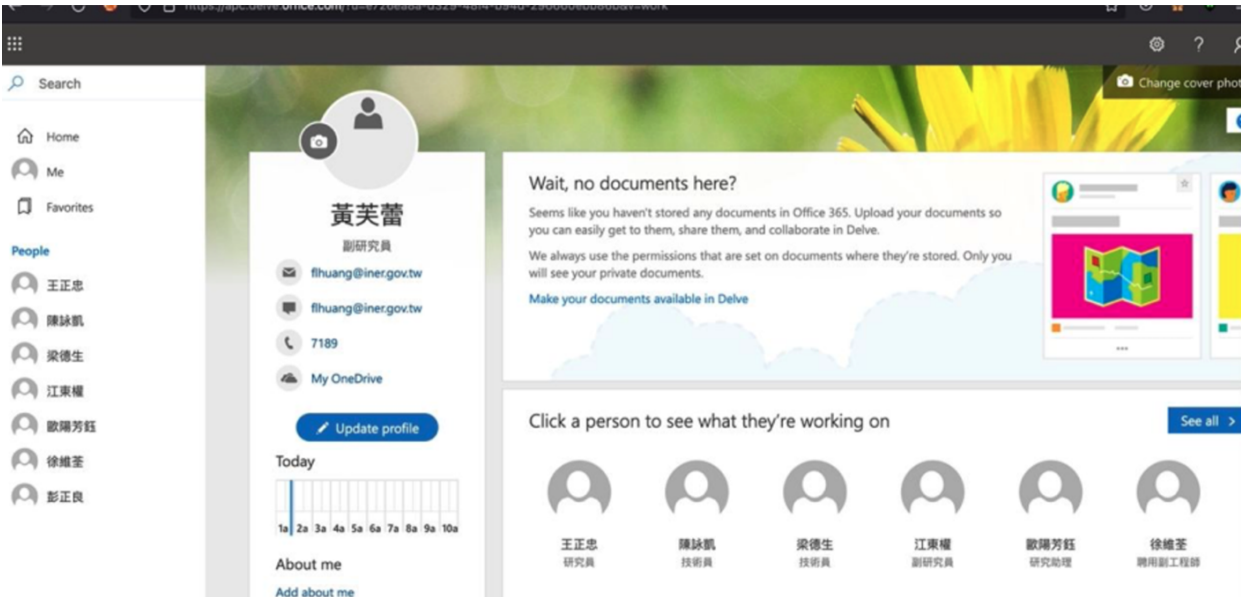
Notably, 'SKS3001', the threat actor who posted the 15GB leak of Rosatom data, appears to be a native Spanish speaker, although the posting language could have just been an OPSEC tactic used by the leaker to drop a 'red herring' for incident responders. Beyond ROSATOM, this leak also contained documents and data

related to Techsnabexport (TENEX), another Russian state-owned company that exports enriched Uranium to global customers.

Rosatom
gigabytes of files allegedly hacked from the Rosatom State Nuclear Energy Corporation, including information on Techsnabexport / Техснабэкспорт, commonly known as TENEX, which exports uranium and provides uranium enrichment services for foreign reactors. Rosatom is responsible for 76% of global nuclear technology exports.
The files include over 10,000 photographs, over 1,000 documents, numerous files from the websites, and SQL files from 2020.
Country: Russia
Size: 15 GB

Taiwan’s Institute Of Nuclear Energy Research (INER)

Resecurity has discovered that an IAB has been selling access to Taiwan’s Institute of Nuclear Energy Research (INER) through a compromised employee’s Office 365 account. The threat actor was monetizing the stolen INER credentials through a trusted network of contacts in the underground cybercriminal network. This same IAB was also found to be selling access to other nuclear research organizations in Thailand, Vietnam, Brunei, and Malaysia in 2022. We have shared this information with Taiwanese authorities and U.S. law enforcement partners.



Compromised Office 356 account.

1.RDP
Revenue : 50kk
Country : Chile
Industry : Insurance and leasing
Local Administrator rights
AV : Sophos
Price : 1000\$

2. Psexec connection inside
Revenue : 5kk
Country : Canada
Industry : Energy
Local Administrator rights
AV : Malwarebytes
Price : 1000\$

Dealing only with people with reputation from the forum or users that have deposits , new users i ignore

Escrow accepted

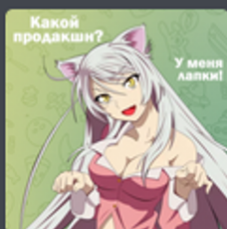
faggotron and d0p

Threat actor ‘in the matrix’ sells admin-level access to a Canadian energy firm, source: RAMP.

Sell access on corp width 143kk revenue

w1nte4mute · Apr 13, 2022

Forums > Market \ 市场 > Access (SSH/RDP/VNC/Shell) \ 访问



w1nte4mute

Member

Dec 14, 2021

Messages 30

Reaction score 5

Points 8

Apr 13, 2022

I sell vnc/rdp access to the company.

Country: **India**

Revenue: **143kk**

Direction: **Production of energy industry equipment.**

Price: **15-20k**

//conditions can be discussed in pm 🙄

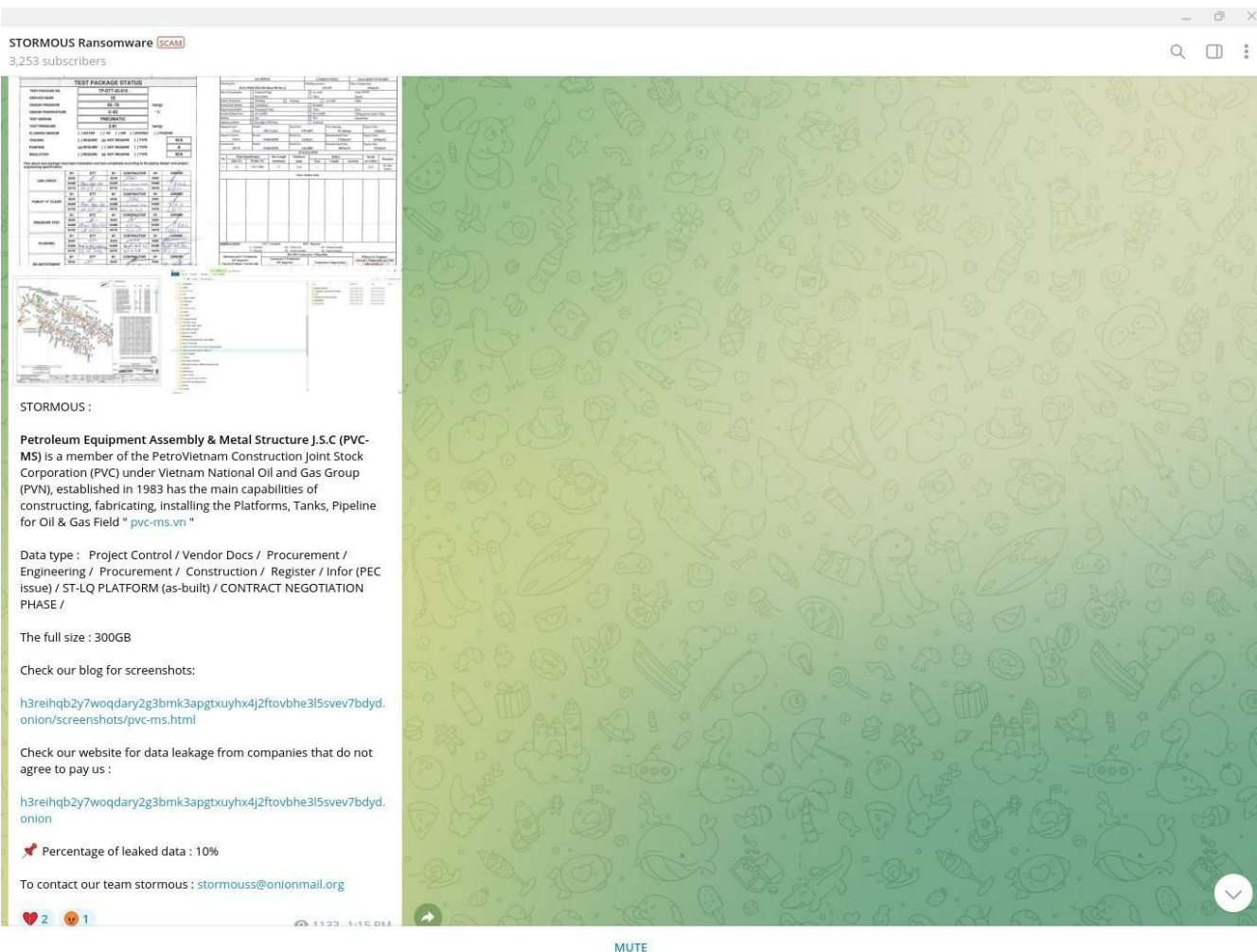
Only the guarantor.

Reply

Threat actor 'w1nte4mute' sells access to an Indian producer of energy industry equipment, source: RAMP.

STORMOUS Announces the Compromise of Petroleum Equipment Assembly & Metal Structure J.S.C (PVC-MS) in Vietnam

On September 7, 2023, the pro-Russian 'STORMOUS' ransomware gang announced on their official Telegram channel that they had compromised 300 GB of Petroleum Equipment Assembly & Metal Structure J.S.C (PVC-MS) data. This victim entity is a "member of the PetroVietnam Construction Joint Stock Corporation (PVC) under Vietnam National Oil and Gas Group (PVN), established in 1983. It has the main capabilities of constructing, fabricating, and installing the Platforms, Tanks, and Pipeline for Oil & Gas Fields," according to the victim's website.



STORMOUS announces the compromise of 300 GB of PVC-MS data, source: Telegram.

Per STORMOUS' Telegram posting, data types they stole from PVC-MS include: "Project Control / Vendor Docs / Procurement / Engineering / Procurement / Construction / Register / Infor (PEC issue) / ST-LQ PLATFORM (as-built) / CONTRACT NEGOTIATION PHASE." STORMOUS has leaked just 10% of the 300 GB PVC-MS data dump.

STORMOUS' attack on PVC-MS is also in line with threats the group made back in May 2022 after returning from a short hiatus. The group published a message on Telegram: "We will promise that we will destroy all the different companies in the USA, the country of Vietnam, and Peru." See the screenshot below.



STORMOUS Ransomware SCAM
2,690 subscribers



Dear followers we are back with a message for you

After we finished planning we came to the useful conclusion that we will promise that we will destroy all the different companies in the USA the country of Vietnam and the country of Peru

we will publish their lies and perhaps get special permission to enter the Peru government to publish large samples of sensitive information about their country and expose the lies of this particular country We will confiscate all their data and the entire lives of government members in a pdf file and their files will be private and confidential Do they support terrorism ? Sorry we've gotten into the details but we promise in a few months we'll publish everything for you.

As for the United States of America we have not forgotten it We also added (Vietnam and Peru) to the victims
[#wait for us](#)



STORMOUS announces their targeting of the USA, Vietnam, and Peru, source: Telegram.

In July 2022, STORMOUS followed up this announcement with another Telegram post, specifying the geopolitical considerations guiding their target selection. They quantified their target criteria as follows: America (80%), Ukraine (60%), India (58%), Peru (50%), and Vietnam (12%). See the screenshot below.



STORMOUS Ransomware

Welcome !

We'll tell you a little something this new month that we'll do well! We are designing our own ransomware (StormousX) which will be a corporate hell! Another point, we will launch our dark web site (.onion) this month and it will look like this:
Publishing and leaking victim data

We will tell you if only the victim's data was stolen or a ransomware was released (this is just to see if the data alone was stolen or a ransomware was released)

There is also a shop where we can sell the data of some important companies!
A site will be opened these days and we will tell you many things !

Our own goals ! :

(America 80% _ Ukraine 60% _ India 58% _ Peru 50% _ Vietnam 12%)
We will focus on these goals well!

As for the distribution of the data, it will be good and the data will be published in full, and in terms of credibility, I do not care. If you are really an expert! You can check if the data is correct and if there is a breach because we really don't waste our time discussing a stupid case what can we gain from this fraud! Let's not discuss this issue. deception channel. It's just made by US companies to stop us !

About this in a report from India about the latest data theft attack * on a large number of their companies by us :

<https://www.livemint.com/technology/tech-news/indian-companies-in-ransomware-group-s-radar-claims-report/amp-11656673183695.html>

Reply : You are at war, we don't care, we will continue to attack your companies, maybe half of the data published on our site is data from your own companies which you will see soon!

Brown might have won. You will see their full data leaked on our new website which will be launched soon

STORMOUS explains their geopolitical targeting priorities, source: Telegram.

“Big Game” Hunting – Black Basta Targets the Energy Sector

Among active ransomware crews targeting the energy sector, Black Basta is one of today's most prolific threat groups. First identified in the wild in 2022, Black Basta is believed to be a splintered ‘rebrand’ of the now-dissolved ransomware syndicate Conti. The group’s tactics, techniques, and procedures (TTPs) also overlap specific attack signatures observed in breaches attributed to BlackMatter.

Resecurity has recently identified an updated Black Basta ransomware variant that has targeted multiple entities operating in the European energy sector. Black Basta distributed the new attack variant to their affiliates sometime in February and then released a version update around March 10. Around this time, Black Basta operators were demanding \$6 million from one energy company victim in the EU and another \$3.5 million from a logistics company in the Nordic region that provides transport services for the oil & gas industry.

The identities of these victims have not been disclosed on Black Basta’s DLS.

One of the most significant upgrades to the previous Black Basta ransomware version is the new variant’s optimized encryption library. Black Basta developers replaced the Mini-GMP code library used in the older versions (<https://github.com/idris-lang/ldris-dev/blob/master/rt/mini-gmp.c>) with the Cryptoapp (<https://github.com/weidai11/cryptopp>) library. Another enhancement observed in one variant update distributed to a specific affiliate includes a customized package containing a ‘cryptor’ malware obfuscation tool and several .bat files used for anti-virus evasion/deactivation.

<https://twitter.com/FalconFeedsio/status/1630091991810801666>

This BlackBasta ransomware strain was written in C++ and compiled for Win32.

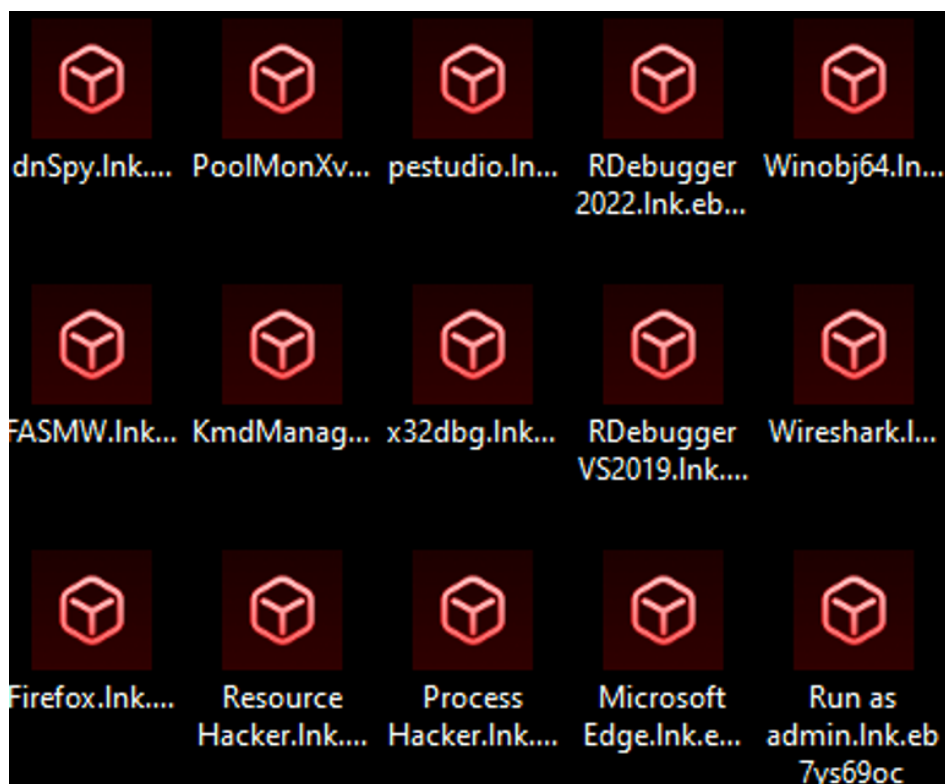
Files:

- av.bat – performs a hidden deletion of an application with the given GUID: {7E4BEC2F-7D16-4A7D-9174-BE810D60A187}
- av1.bat – performs a hidden deletion of an application with the given GUID: {C8902761-479E-4590-A707-6623FCC66FA6}
- sym.bat – runs smc.exe with the -stop parameter (Looks like Symantec Endpoint Protection is disabled)
- TI_c.exe is a cryptor that hides as the Symantec Norton Security with Backup Portable Restore Utility.
- TI_c.dll is a library version of the TI_c.exe cryptor.
- S2.exe – knocks via TCP by the address from files list_x...

Algorithm Functionality

When we ran the TI_c.exe, the encryption process started. The encrypted files have the “.eb7ys69oc” extension (see Figure 0). Once the data is encrypted, this strain generates a “read-me” file in each folder (see Figure 1). This file includes a link to Black Basta’s dark web chat site (see Figure 2 and Figure 3).

Reference: <https://bastad5huzwkepdixedg2gek7jk22ato24zylp6lnjx7wdtyctgvvd.onion/>



Encrypted files.

instructions_read_me - Notepad
File Edit Format View Help

ATTENTION!
Your network has been breached and all data was encrypted. Please contact us at:
<https://bastad5huzwkepdixedg2gek7jk22ato24zylp6lnjx7wdtyctgvvd.onion/>

Login ID: e281533c-2472-4751-b7d0-8b753f36076b

**** To access .onion websites download and install Tor Browser at:**
<https://www.torproject.org/> (Tor Browser is not related to us)

**** To restore all your PCs and get your network working again, follow these instructions:**

- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.

Please follow these simple rules to avoid data corruption:

- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption.
- Do not hire a recovery company. They can't decrypt without the key. They also don't care about your business. They believe that they are good negotiators, but it is not. They usually fail. So speak for yourself.

Waiting you in a chat.

Figure 1 – File with instructions left for the victim (instructions_read_me.txt)

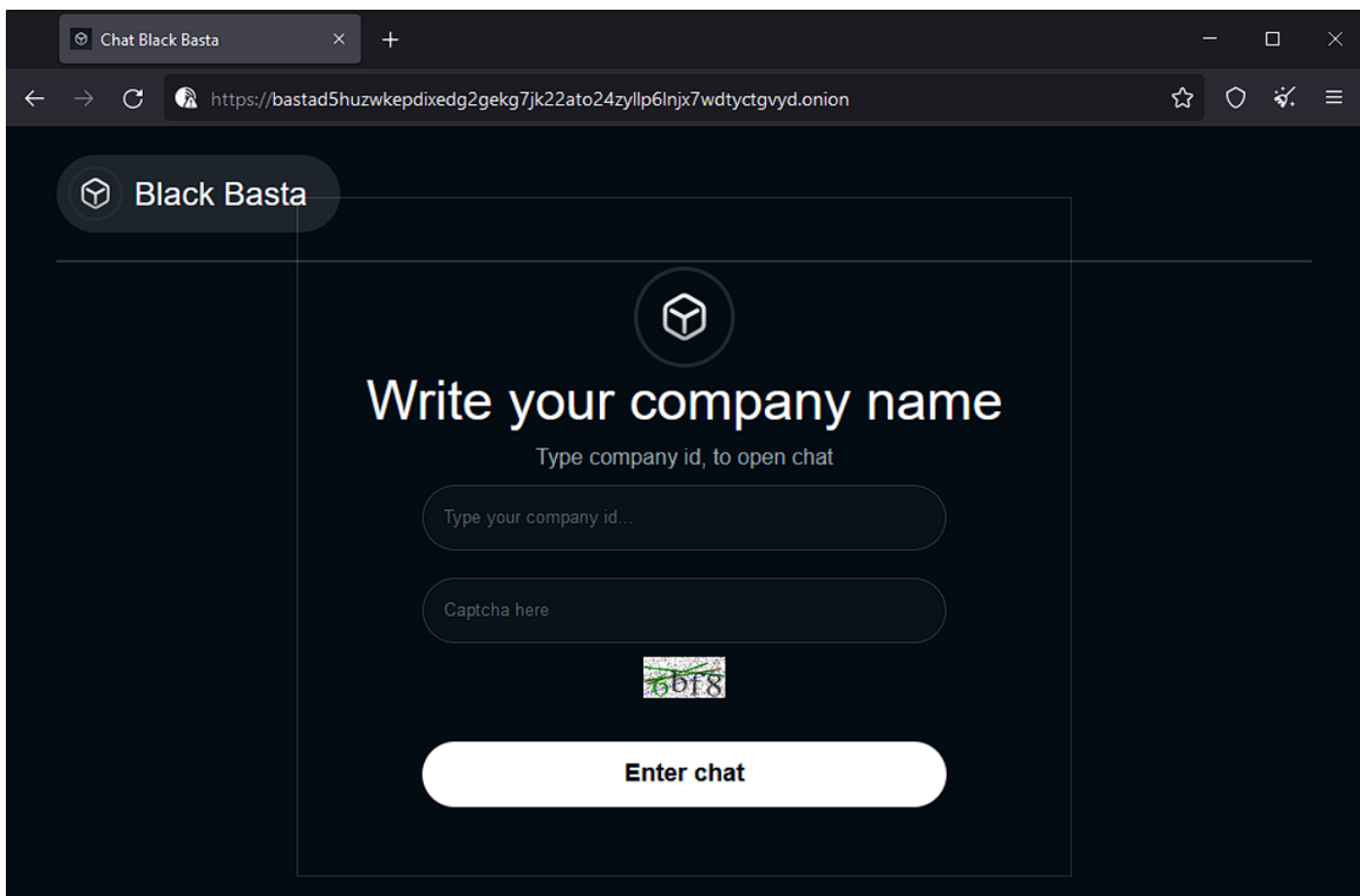


Figure 2 – Per the instructions, the website is to pay the ransom with authorization by ID.

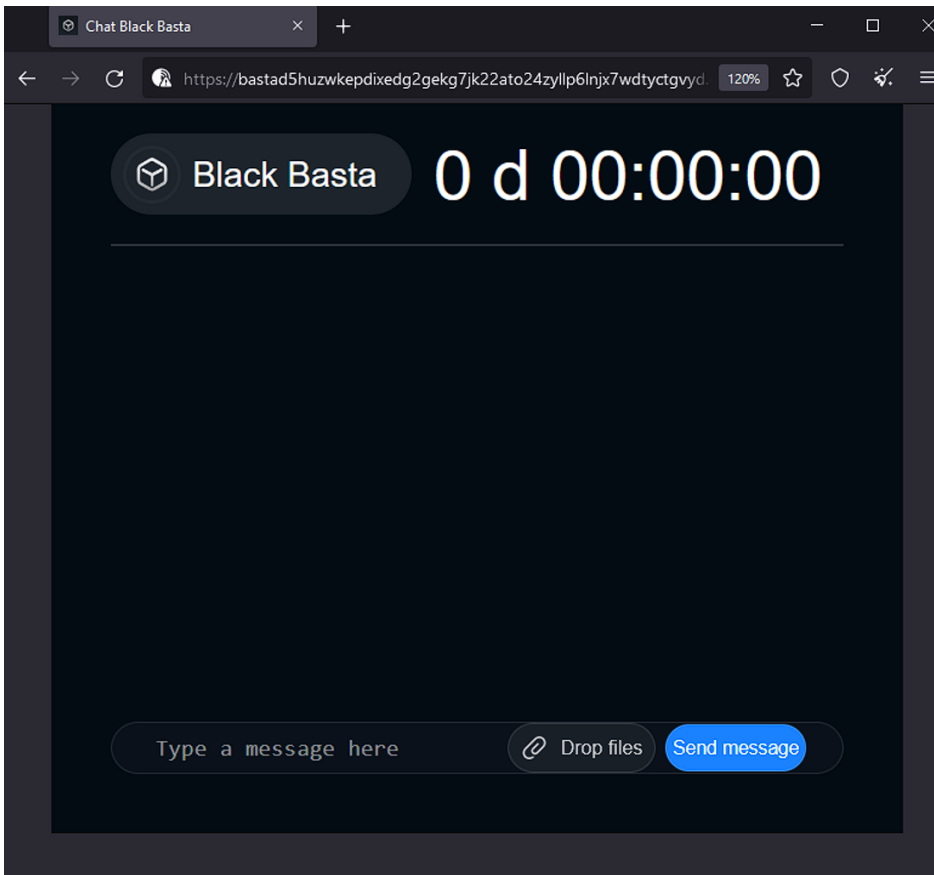


Figure 3 – Per the instructions, the Black Basta chat to pay the ransom with authorization by ID.

Cybercriminal Negotiations

In Figure 4, Resecurity investigators pretended to be a regular employee whose laptop data had been encrypted. They contacted Black Basta's customer support team to inquire about the cost of decrypting the ransomed files.



Figure 4 – Initial communication via the Black Basta chat.

Afterward, Black Basta instructed our investigator to go to another chat by copying the Chat ID from a Privnote message. Privnote is a self-destructive messaging app popular in the cybercriminal underground (see Figure 5). When our investigator resumed the chat, a timer began, and Black Basta’s support team instructed them to make a ransom payment of \$5 million (refer to Figure 6.1 and Figure 6.2).

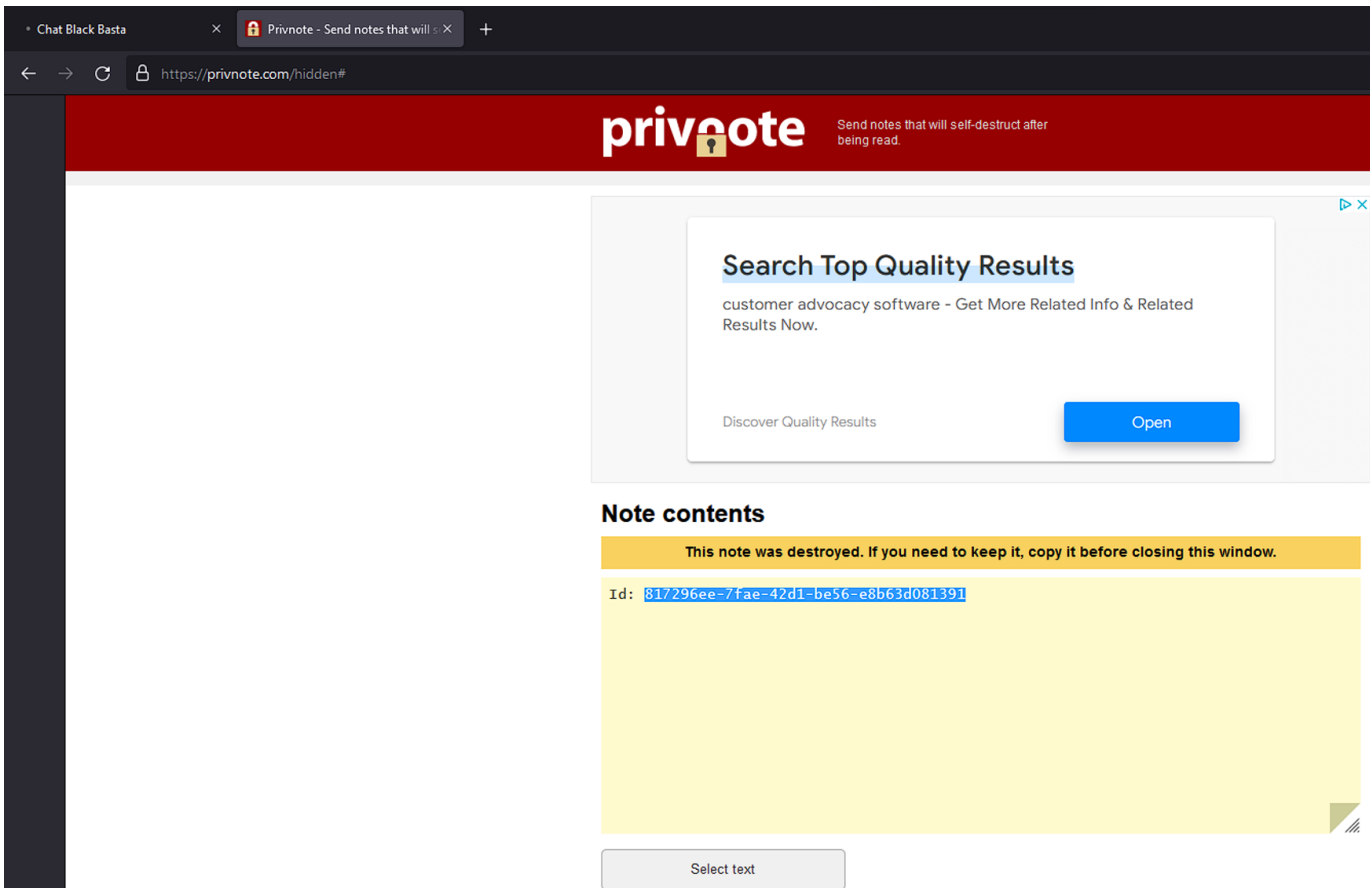


Figure 5 – Privnote referenced in Figure 4.

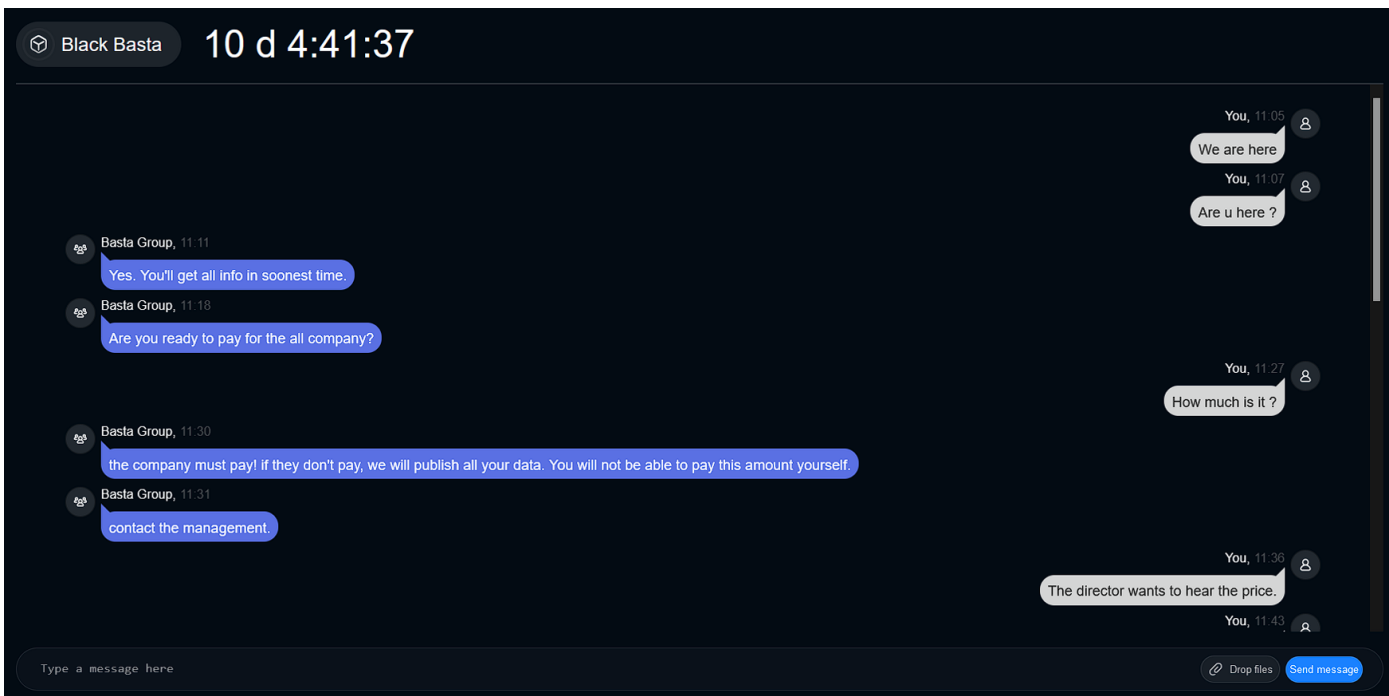


Figure 6.1 – Ransom demand.

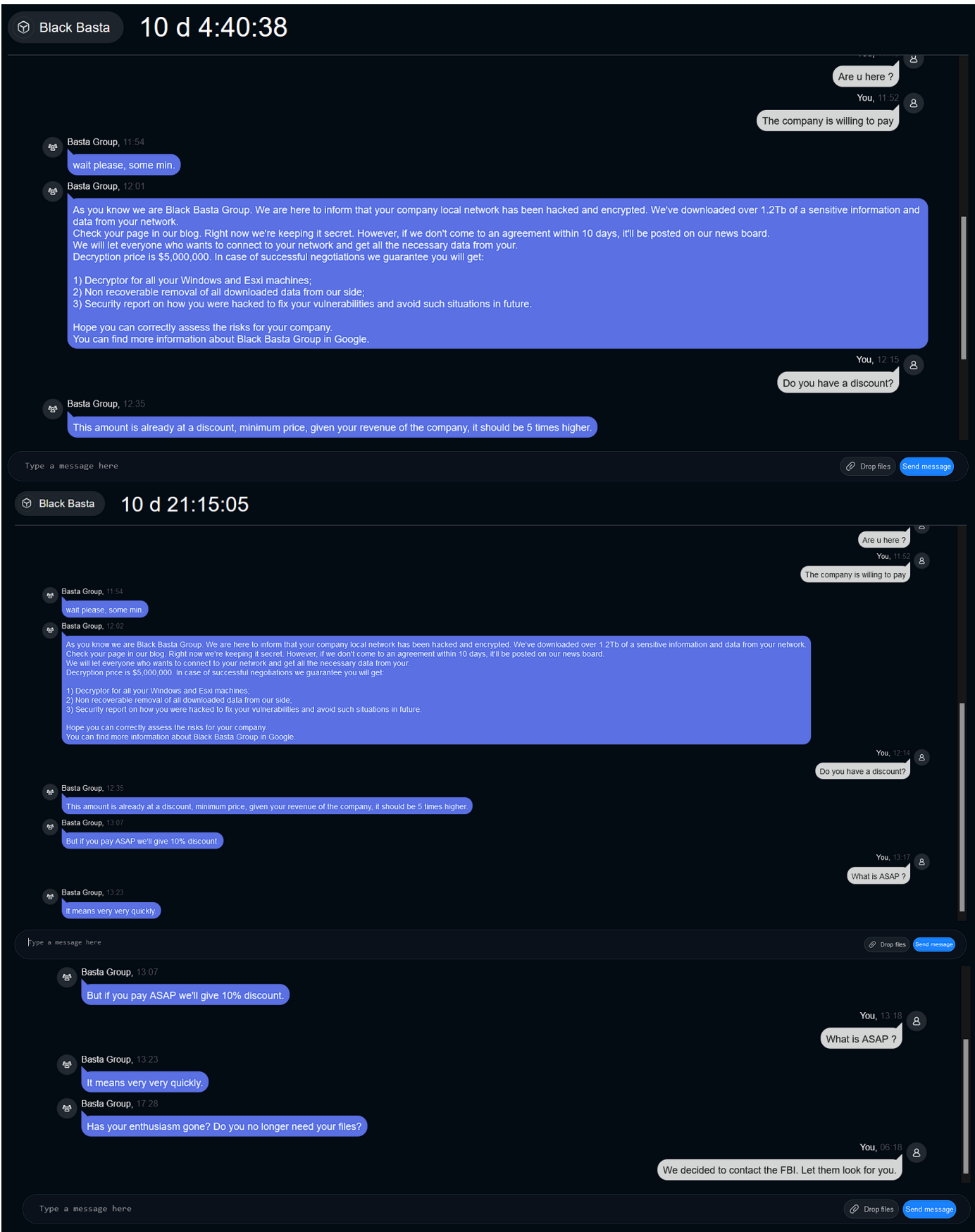


Figure 6.2 – Ransom demand.

Analysis of S2.exe

MD5: 6f20f5aa2eb7a0c53a39b49024d938ee

SHA256: a9dd4eae8612729957bfeac53b764aba6243c749c7b7666e21acec1504efde84

SHA512:

188b46145135c5f850ac811975cc87f07a5493ee4d6c41db6ec361da5445b4e3b00964c7a691e4ab520dd2b88
ed0a60969c43599a0d22b2b9f645f7250bc7e98


This module, called s2.exe, is encrypted and uses an anti-debugging technique. After unpacking it, we found that it sends a signal via TCP to the addresses listed in files list_0, list_1, and so on (see Figures 9 and 10). However, this module's execution needs to be clarified since the cryptor process does not activate it. See Figure 7 and Figure 8 for more details.


Name	Base address	Size	Description
s2.exe	0x400000	39.63 ...	
advapi32.dll	0x75500000	488 kB	Advanced Windows 32 Base...
apphelp.dll	0x73940000	636 kB	Application Compatibility Clie...
bcryptprimitives...	0x76ee0000	380 kB	Windows Cryptographic Pri...
combase.dll	0x75890000	2.5 MB	Microsoft COM for Windows
CoreMessaging.dll	0x73fa0000	620 kB	Microsoft CoreMessaging Dll
CoreUICompon...	0x74040000	2.49 MB	Microsoft Core UI Compone...
gdi32.dll	0x75df0000	144 kB	GDI Client DLL
gdi32full.dll	0x77130000	880 kB	GDI Client DLL
imm32.dll	0x750e0000	148 kB	Multi-User Windows IMM32 ...
kernel.appcore.dll	0x73ae0000	60 kB	AppModel API Host
kernel32.dll	0x757a0000	960 kB	Windows NT BASE API Clie...
KernelBase.dll	0x75580000	2.08 MB	Windows NT BASE API Clie...
locale.nls	0x2bb00000	804 kB	
msctf.dll	0x76340000	844 kB	MSCTF Server DLL
msimg32.dll	0x745c0000	24 kB	GDIEXT Client DLL
msvc_p_win.dll	0x770a0000	492 kB	Microsoft® C Runtime Library
msvcr100.dll	0x744e0000	764 kB	Microsoft® C Runtime Library
msvcr.dll	0x75320000	764 kB	Windows NT CRT DLL
mswsock.dll	0x73420000	328 kB	Microsoft Windows Sockets ...
ntdll.dll	0x77220000	1.64 MB	NT Layer DLL
ntdll.dll	0x7fff97d9...	1.96 MB	NT Layer DLL
ntmarta.dll	0x744b0000	164 kB	Windows NT MARTA provider
oleaut32.dll	0x75110000	600 kB	OLEAUT32.DLL
rpcrt4.dll	0x76280000	764 kB	Remote Procedure Call Runt...
sechost.dll	0x75ba0000	468 kB	Host for SCM/SDDL/LSA Loo...
secur32.dll	0x745a0000	40 kB	Security Support Provider In...
SHCore.dll	0x753e0000	540 kB	SHCORE
SortDefault.nls	0x4d600000	3.22 MB	
sspicli.dll	0x73a30000	132 kB	Security Support Provider In...
TextInputFram...	0x742c0000	740 kB	"TextInputFramework.DYNL...
ucrtdbase.dll	0x75c20000	1.13 MB	Microsoft® C Runtime Library
user32.dll	0x76d40000	1.63 MB	Multi-User Windows USER A...
uxtheme.dll	0x74380000	464 kB	Microsoft UxTheme Library
win32u.dll	0x765e0000	96 kB	Win32u
WinTypes.dll	0x73ec0000	876 kB	Windows Base Types DLL
wow64.dll	0x7fff96f4...	356 kB	Win32 Emulation on NT64
wow64cpu.dll	0x77210000	40 kB	AMD64 Wow64 CPU
wow64win.dll	0x7fff9750...	524 kB	Wow64 Console and Win32 ...
ws2_32.dll	0x76640000	396 kB	Windows Socket 2.0 32-Bit DLL
wsock32.dll	0x745b0000	32 kB	Windows Socket 32-Bit DLL


Figure 7 – The s2.exe modules.


registry	-	-	RegCloseKey
registry	-	-	RegCreateKeyEx
registry	Modify Registry	Defense Evasion	RegDeleteValue
registry	-	-	RegOpenKeyEx
registry	Modify Registry	Defense Evasion	RegSetValueEx
registry	-	-	WritePrivateProfileString
network	-	-	WSAStartup
network	-	-	closesocket
network	-	-	connect
network	-	-	htons
network	-	-	ioctlsocket
network	-	-	recv
network	-	-	send
network	-	-	setsockopt
network	System Shutdown/R...	Persistence	shutdown
network	-	-	socket
network	-	-	wsock32.dll
network	-	-	WSAIoctl
network	-	-	freeaddrinfo
network	-	-	getaddrinfo
network	-	-	ws2_32.dll

Figure 8 – APIs that use the s2.exe.

 Event Properties

 Event

 Process

 Stack

Date: 2/20/2023 10:14:32.2592600 AM

Thread: 0

Class: Network

Operation: TCP Disconnect

Result: SUCCESS

Path: DESKTOP-UOG5TGB.localdomain:60779 -> 89.185.85.249:https

Duration: 0.0000000

Length: 0

seqnum: 0

connid: 0

Figure 9 – The signal being sent to the malicious server.

```

553 92.111873 192.168.88.135 89.185.85.249 TCP 66 49831 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
554 93.112571 192.168.88.135 89.185.85.249 TCP 66 [TCP Retransmission] [TCP Port numbers reused] 49831 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
555 93.138634 89.185.85.249 192.168.88.135 TCP 64 443 → 49829 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
556 95.113560 192.168.88.135 89.185.85.249 TCP 66 [TCP Retransmission] [TCP Port numbers reused] 49831 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

```

```

> Frame 556: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface Device\NPF_{95A802D8-86D6-4842-8477-A7982E6D1E75}, id 0
> Ethernet II, Src: VMware_46:1d:17 (00:0c:29:46:1d:17), Dst: VMware_eb:d2:93 (00:50:56:eb:d2:93)
> Internet Protocol Version 4, Src: 192.168.88.135, Dst: 89.185.85.249
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 52
  Identification: 0x4d44 (19780)
  > Flags: 0x40, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0xe49d [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.88.135

```

```

0000 00 50 56 eb d2 93 00 0c 29 46 1d 17 08 00 45 00 PV.....)F....E.
0010 00 34 4d 44 40 00 00 06 4d 0c c0 a8 58 87 59 b9 4ND@...  X.Y.
0020 55 f9 c2 a7 01 bb 15 0f d1 31 00 00 00 00 02 0 U.....1.....
0030 fa f0 00 9a 00 00 02 04 05 b4 01 03 03 08 01 01 .....
0040 04 02 ..

```

Figure 10 – Requests that are sent to the malicious server.

Analysis of TI_c.exe

MD5: 2f4acd97542131cda5f26249176348e3

SHA256: b0e43793c527802856bfa3a81b02b3f10e29d74fc60d8b233247a42f0cbc78eb

SHA512:

f0ed9685e85f0e8d8ce7324f7a5813db2bf08021e102b758dd88dbf5b450fb139f3116db5029bf11f2b548f17be89e42e2a3d84c07ca64ffbc3cab2a1fb04c43

The TI_c.exe executable is a cryptor. First, it collects file information and then starts the encryption process. After the files have been encrypted, this image is unloaded from memory.

The cryptor ignores the following folders: C:\Windows, C:\Program Files, C:\Program Files (x86), and \$Recycle Bin.

The cryptor works with the registry to create the registry key: “HKCR\eb7ys69oc\”. (See Figure 11).

The cryptor has a bug that sometimes encrypts its icon (See Figure 12).

Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions	0xb4
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale	0xc4
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	0xe4
Key	HKLM	0x100
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Ids	0x12c
Key	HKLM	0x138
Key	HKLM\SOFTWARE\Microsoft\Ole	0x13c
Key	HKLM\SYSTEM\ControlSet001\Control\Session Manager	0x1ac
Key	HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion	0x330
Key	HKCR\eb7ys69oc\DefaultIcon	0x378
Key	HKCU\Software\Classes	0x3d0

Figure 11 – Malware-compatible registry keys.

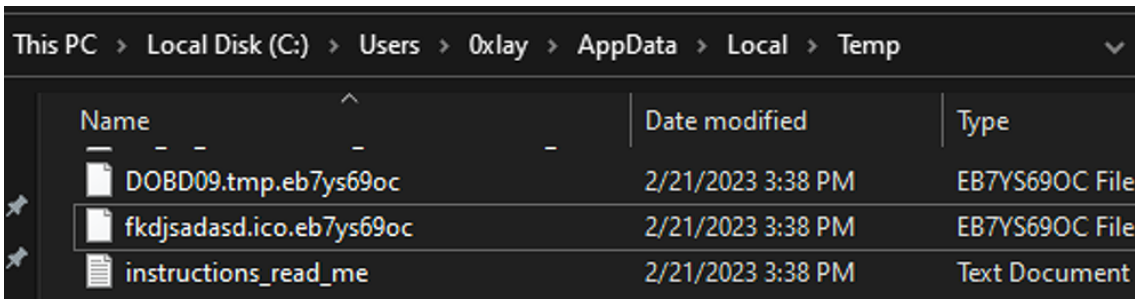


Figure 12 –Self-encrypting icon.

The cryptor spawns the process “vssadmin.exe” to delete snapshots (see Figure 13). The “vssadmin.exe” is a command-line utility found in all Microsoft Windows operating systems after Windows XP. This utility manages the Volume Shadow Copy Service (VSS), a Windows service that allows users to create and manage snapshots of volumes for backup and restore purposes.

```

debug063:0340410E loc_340410E:                ; CODE XREF: sub_3403F80+1D↑j
debug063:0340410E                push    offset aWmStarted ; "Wm started\n"
debug063:03404113                call   maybe_fwrite
debug063:03404118                push    offset aCWindowsSysnat ; "C:\\Windows\\SysNative\\vssadmin.exe de"
debug063:0340411D                call   SpawnProcess |
debug063:0340412A                mov     ecx, [ebp+var_4]
debug063:0340412A                db     'C:\\Windows\\SysNative\\vssadmin.exe delete shadows /all /quiet',0
debug063:0340412A                ; DATA XREF: sub_3403F80+198↑o

```

Figure 13 – Deleting snapshots.

The cryptor acquires data on files by utilizing the FindFirstFileA and FindNextFileA APIs (see Figure 14) as well as FindFirstVolumeW and FindNextVolumeW functions, which are Windows APIs that provide handles for volumes on a computer (see Figure 15).

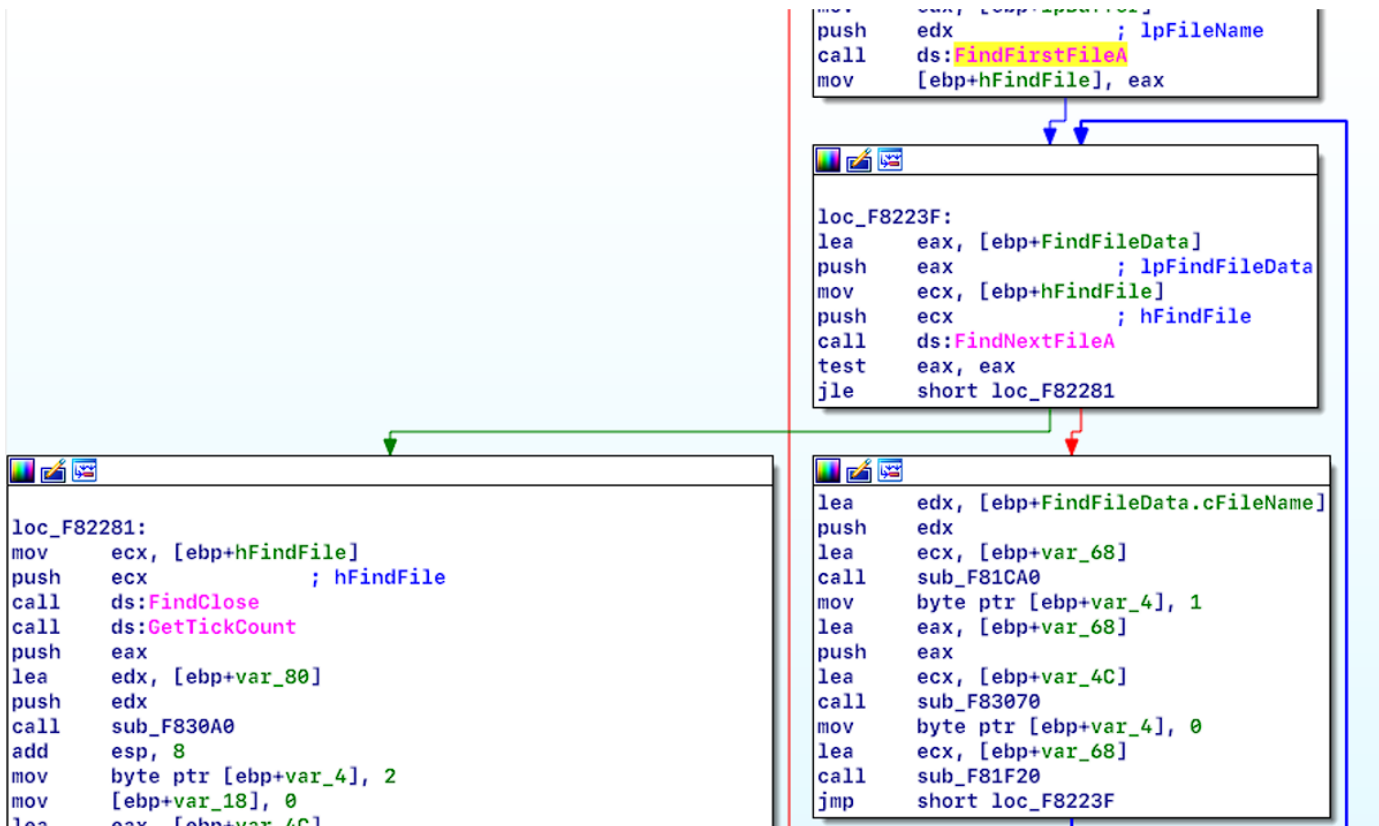


Figure 14 – Collecting information about the victim’s files.

```

debug065:036143CF mov     dword ptr [ebp-4], 0
debug065:036143D6 push    eax
debug065:036143D7 mov     dword ptr [ebp-0C2Ch], 1
debug065:036143E1 call   offset_kernel32_FindFirstVolumeW
debug065:036143E7 mov     edi, eax
debug065:036143E9 nop     dword ptr [eax+00000000h]

```

Figure 15 – Collecting information about volumes.

After unpacking, Resecurity investigators found that the cryptor was using the CryptoPP library (see Figure 16) (<https://github.com/weidai11/cryptopp>). Next, we found that the chacha20 algorithm was used for encryption (see Figure 17).

0349CAB0	17	M	CryptoPP::SymmetricCipherFinal<...	CryptoPP::SymmetricCipherFi
0349CAF8	16	M	CryptoPP::SymmetricCipherFinal<...	CryptoPP::StreamTransforma
0349CB3C	12	M	CryptoPP::SymmetricCipherFinal<...	CryptoPP::RandomNumberGe
0349CB70	13	M	CryptoPP::SymmetricCipherFinal<...	CryptoPP::XChaCha20_Policy
0349CBA8	3		CryptoPP::DL_KeyAgreementAlgo...	CryptoPP::DL_KeyAgreement
0349CBB8	3		CryptoPP::DL_KeyDerivationAlgor...	CryptoPP::DL_KeyDerivation
0349CBC8	7		CryptoPP::DL_EncryptionAlgorith...	CryptoPP::DL_EncryptionAlgo

Figure 16 – The CryptoPP library.

```

debug063:0340B556      push    eax
debug063:0340B557      lea    ecx, [edi+4]
debug063:0340B55A      call   CryptoPP::AdditiveCipherTemplate<CryptoPP::AbstractPolicyHolder<CryptoPP::AdditiveCipherAbstractPolicy, CryptoPP::SymmetricCipher>>::f
debug063:0340B55F      lea    eax, [ebp+var_28]
debug063:0340B562      push    eax
debug063:0340B563      push    0
debug063:0340B565      push    [ebp+arg_C]
debug063:0340B568      push    [ebp+var_10]
debug063:0340B56B      push    esi
debug063:0340B56C      call   kernel32_WriteFile
debug063:0340B572      push    [ebp+var_10]
debug063:0340B575      call   operator_delete[](void *)
debug063:0340B57A      mov     eax, edi
debug063:0340B57C      mov     dword ptr [edi+4], offset const CryptoPP::SymmetricCipherFinal<CryptoPP::ConcretePolicyHolder<CryptoPP::XChaCha20_Policy, CryptoPP::At
debug063:0340B583      add     esp, 4
debug063:0340B586      mov     ecx, eax
debug063:0340B588      mov     dword ptr [eax], offset const CryptoPP::SymmetricCipherFinal<CryptoPP::ConcretePolicyHolder<CryptoPP::XChaCha20_Policy, CryptoPP::Addi
debug063:0340B58E      mov     dword ptr [eax+8], offset const CryptoPP::SymmetricCipherFinal<CryptoPP::ConcretePolicyHolder<CryptoPP::XChaCha20_Policy, CryptoPP::At
debug063:0340B595      mov     dword ptr [eax+20h], offset const CryptoPP::SymmetricCipherFinal<CryptoPP::ConcretePolicyHolder<CryptoPP::XChaCha20_Policy, CryptoPP::At
debug063:0340B59C      call   sub_3407330
debug063:0340B5A1      mov     ecx, [ebp+var_C]
debug063:0340B5A4      mov     large fs:0, ecx
debug063:0340B5AB      pop     ecx
debug063:0340B5AC      pop     edi
debug063:0340B5AD      pop     esi
debug063:0340B5AE      mov     esp, ebp
debug063:0340B5B0      pop     ebp
debug063:0340B5B1      retn   18h

```

Figure 17 – Using the chacha20 algorithm.

Each encrypted file stores the string “1te1qivtlse” at the end of the cipher. (See Figure 18)

```

00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 d1 | .....Ñ
00 31 74 65 | 31 71 69 76 | 74 6c 73 65 | 00  _   |               |               |               |               |               |

```

Figure 18 – The magic string.

We encrypted a file that was 959B in size and found that 64B were skipped while 896B were successfully encrypted, as shown in Figure 19. However, when the file was larger than 4KB, we noticed that 64B were encrypted while 128B were skipped, as depicted in Figure 20.

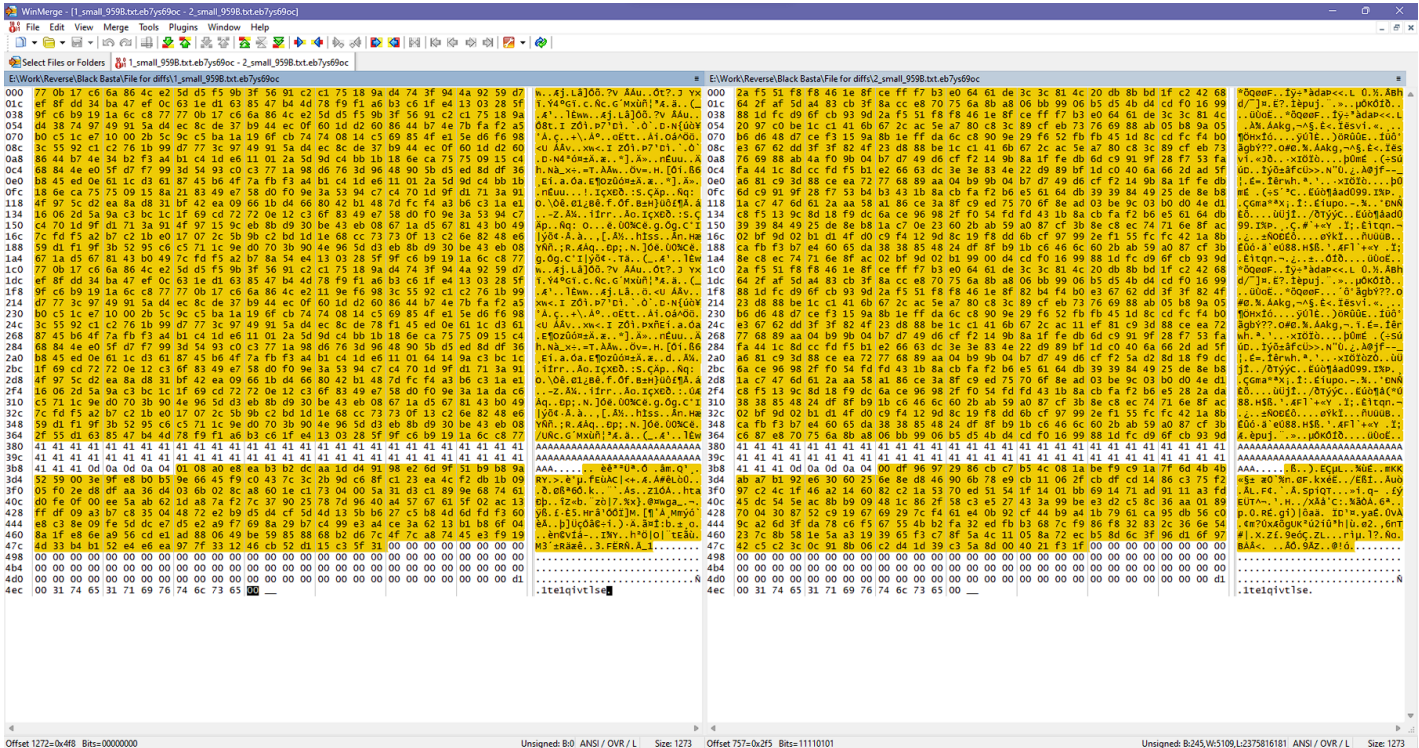


Figure 19 – Small encrypted file.

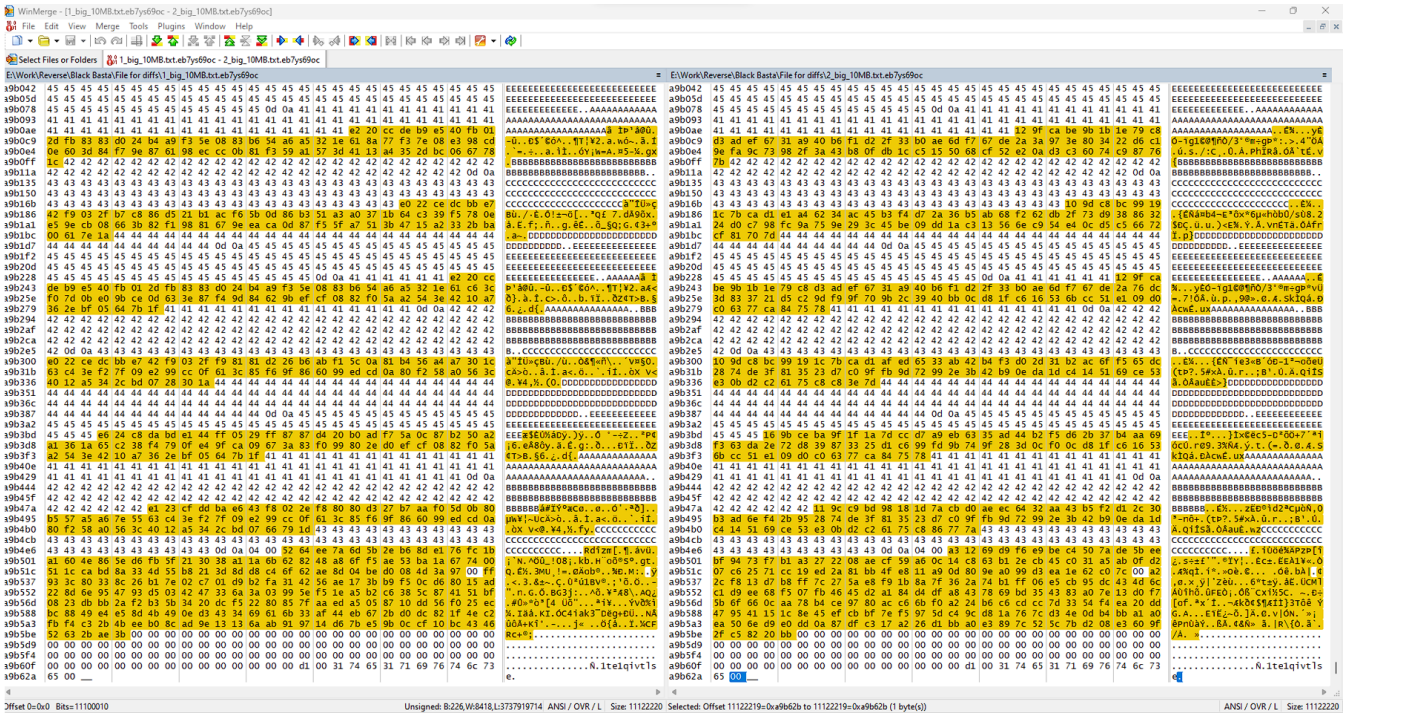


Figure 20 – Large encrypted file.

TI_c.exe (6116) Properties

General Statistics Performance Threads **Token** Modules Memory Environment Handles GPU Disk and Network Comment

User: DESKTOP-UJOG5TGB\0xlay
 User SID: S-1-5-21-367392591-3648379057-2715769128-1000
 Session: 1 Elevated: Yes Virtualized: Not allowed
 App container SID: N/A

Name	Flags
BUILTIN\Administrators	Mandatory (default enabled)
BUILTIN\Users	Mandatory (default enabled)
CONSOLE LOGON	Mandatory (default enabled)
DESKTOP-UJOG5TGB\None	Mandatory (default enabled)
Everyone	Mandatory (default enabled)
LOCAL	Mandatory (default enabled)

Name	Status	Description
SeBackupPrivilege	Disabled	Back up ...
SeChangeNotifyPrivilege	Default Enabled	Bypass t...
SeCreateGlobalPrivilege	Default Enabled	Create g...
SeCreatePagefilePrivilege	Disabled	Create a...
SeCreateSymbolicLinkPrivilege	Disabled	Create s...
SeDebugPrivilege	Disabled	Debug p...
SeDelegateSessionUserImpersonatePrivilege	Disabled	Obtain a...
SeImpersonatePrivilege	Default Enabled	Imperso...
SeIncreaseBasePriorityPrivilege	Disabled	Increase...
SeIncreaseQuotaPrivilege	Disabled	Adjust m...
SeIncreaseWorkingSetPrivilege	Disabled	Increase...
SeLoadDriverPrivilege	Disabled	Load an...
SeManageVolumePrivilege	Disabled	Perform ...
SeProfileSingleProcessPrivilege	Disabled	Profile si...
SeRemoteShutdownPrivilege	Disabled	Force sh...
SeRestorePrivilege	Disabled	Restore ...
SeSecurityPrivilege	Disabled	Manage ...
SeShutdownPrivilege	Disabled	Shut do...
SeSystemEnvironmentPrivilege	Disabled	Modify fi...
SeSystemProfilePrivilege	Disabled	Profile s...
SeSystemtimePrivilege	Disabled	Change ...
SeTakeOwnershipPrivilege	Disabled	Take ow...
SeTimeZonePrivilege	Disabled	Change ...
SeUndockPrivilege	Disabled	Remove ...

Figure 21 – The TI_c.exe privileges.

The cryptor uses the following privileges and modules (see Figure 21 and Figure 22).

Name	Base address	Size	Description
TI_c.exe	0xf80000	964 kB	Norton Security with Bac...
advapi32.dll	0x75500000	488 kB	Advanced Windows 32 Base...
apphelp.dll	0x73a40000	636 kB	Application Compatibility Clie...
bcrypt.dll	0x76260000	100 kB	Windows Cryptographic Pri...
bcryptprimitives...	0x76ee0000	380 kB	Windows Cryptographic Pri...
combase.dll	0x75890000	2.5 MB	Microsoft COM for Windows
cryptbase.dll	0x73d00000	40 kB	Base cryptographic API DLL
cryptsp.dll	0x74680000	76 kB	Cryptographic Service Provi...
gdi32.dll	0x75df0000	144 kB	GDI Client DLL
gdi32full.dll	0x77130000	880 kB	GDI Client DLL
imm32.dll	0x750e0000	148 kB	Multi-User Windows IMM32 ...
kernel.appcore.dll	0x73ae0000	60 kB	AppModel API Host
kernel32.dll	0x757a0000	960 kB	Windows NT BASE API Clie...
KernelBase.dll	0x75580000	2.08 MB	Windows NT BASE API Clie...
locale.nls	0xc80000	804 kB	
msctf.dll	0x76340000	844 kB	MSCTF Server DLL
msvcp_win.dll	0x770a0000	492 kB	Microsoft® C Runtime Library
msvcrt.dll	0x75320000	764 kB	Windows NT CRT DLL
ntdll.dll	0x77220000	1.64 MB	NT Layer DLL
ntdll.dll	0x7fff97d9...	1.96 MB	NT Layer DLL
ole32.dll	0x76420000	908 kB	Microsoft OLE for Windows
oleaut32.dll	0x75110000	600 kB	OLEAUT32.DLL
rpcrt4.dll	0x76280000	764 kB	Remote Procedure Call Runt...
rsaenh.dll	0x73120000	188 kB	Microsoft Enhanced Cryptog...
sechost.dll	0x75ba0000	468 kB	Host for SCM/SDDL/LSA Loo...
SHCore.dll	0x753e0000	540 kB	SHCORE
shell32.dll	0x766b0000	5.7 MB	Windows Shell Common Dll
shlwapi.dll	0x76cf0000	276 kB	Shell Light-weight Utility Libr...
SortDefault.nls	0x2cc0000	3.22 MB	
ucrtbase.dll	0x75c20000	1.13 MB	Microsoft® C Runtime Library
user32.dll	0x76d40000	1.63 MB	Multi-User Windows USER A...
uxtheme.dll	0x74160000	464 kB	Microsoft UxTheme Library
win32u.dll	0x765e0000	96 kB	Win32u
windows.storag...	0x74ad0000	6.03 MB	Microsoft WinRT Storage API
Wldap32.dll	0x76c70000	348 kB	Win32 LDAP API DLL
wldp.dll	0x74aa0000	144 kB	Windows Lockdown Policy
wow64.dll	0x7fff96f4...	356 kB	Win32 Emulation on NT64
wow64cpu.dll	0x77210000	40 kB	AMD64 Wow64 CPU
wow64win.dll	0x7fff9750...	524 kB	Wow64 Console and Win32 ...

Figure 22 – The TI_c.exe modules.

Analyze TI_c.dll

MD5: ca6b2fbb87c4abbbc8202387b1dfc173

SHA256: da6800063764aa4f39998d4aa069ca380ce6bcbe70099e16ece946c1754423cc

SHA512:

0ea3b49bacd9d2b7fbedf0296fdc6cd06c005c54d822a7e9041305c01a01c30a6604fbd17f43aea68716e3fd0639e7f25d76e703843c18d470bdc6930d54ef00

After carefully analyzing both files, we have determined that the TI_c.dll is a version of the TI_c.exe cryptor library (refer to Figure 23 and Figure 24). This library can start the encryption of files by injecting it into a process.

Similarity	Confidence	Change	EA Primary	Name Primary	EA Secondary	Name Secondary
1.00	0.99	-----C	100129F0	StartEncryption	0340AC10	StartEncryption
1.00	0.99	-----C	10074268	__crt_stdio_output::output_processor<char,__crt_st...	0346FB48	sub_0346FB48
1.00	0.99	-----C	10015360	StartAddress	0340D580	ThreadRoutine

Figure 23 – Comparison TI_c.exe and TI_c.dll

Function: MD Index (Call Graph, Bottom Up)	1
Function: MD Index (Call Graph, Top Down)	14
Function: MD Index (Flow Graph MD Index, Top Down)	28
Function: Address Sequence	359
Function: Call Reference	311
Function: Call Sequence (Exact)	6
Function: Call Sequence (Sequence)	43
Function: Edges Call Graph MD Index	105
Function: Edges Flow Graph MD Index	157
Function: Hash	69
Function: Instruction Count	3
Function: Loop Count	1
Function: Name Hash	1940
Function: Prime Signature	95
Confidence	0.991214
Similarity	0.655301

Figure 24 – Comparison statistics.

Summary

The alarming escalation of ransomware attacks against the energy sector and critical infrastructure is a trend that cannot be ignored. With at least a dozen sophisticated groups, such as BlackCat/ALPHV, Medusa, and LockBit 3.0, among others, intensifying their focus on these high-stakes targets, the threat landscape is becoming increasingly dangerous. These threat actors are not acting in isolation; they are supported by a flourishing ecosystem of access brokers and tool developers who provide the necessary leverage to infiltrate and exploit these essential systems. The collaboration between these groups and individual actors indicates the strategic importance placed on the energy sector, which is perceived as a goldmine for high-value data and maximum ransom payouts exceeding \$5,000,000 (million) sometimes.

Looking ahead to 2024, we envision a significant growth in cyber threats, particularly with ransomware groups increasingly prioritizing high-value targets within the energy sector. This specifically focuses on the nuclear energy sector and oil and gas providers in their downstream and upstream operations. As digitalization in these areas continues to advance, the attack surface for malicious actors expands, offering more opportunities for exploitation. While beneficial for operational efficiency, the sector's growing reliance on interconnected technologies presents lucrative opportunities for cybercriminals. The potential for substantial ransom payments, driven by the critical nature of these energy services, further heightens the appeal for these bad actors. Therefore, organizations within these areas of the energy sector must significantly bolster their cyber defenses and prepare for the sophisticated and potentially devastating cyber campaigns that will likely emerge in the coming year.