CYBLE

Underground Threat Activity Report 2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY

CYBLE RESEARCH & INTELLIGENCE LABS (CRIL) closely monitors, tracks, and analyzes cybercrime activities across various underground forums, aka cybercrime forums. This annual report compendiously presents critical cybercrime statistics and trends, vulnerabilities exploited, Tactics, Techniques, and Procedures (TTPs) of Threat Actors from 2022 across various industry sectors and regions to preempt their associated risks.

The previous year's hustle began with a cyber confrontation in the wake of the Russia-Ukraine military conflict. The warfare between the states was joined by several threat actors **(AgainstTheWest, NetSec, GhostSec, Kelvinsecurity, Stormous Ransomware Group, and several nuclear hacktivist groups)** who launched a series of coordinated cyber-attacks from March to September 2022 against private organizations and government establishments to align with their respective allegiances on either side of the conflict. (Ref. 1 & 2)

On the other hand, the **Lapsus$** group carried out a series of cyber-attacks targeting major corporations resulting in some of the biggest data breaches at the beginning of the year. The corresponding risks depicted concerns for the rest of the year which became evident from the back-to-back cyber incidents that followed.

NOTABLE CYBER INCIDENTS 2022

1. NVIDIA Data Leaked by Lapsus$ Group
2. Samsung Data and Source Codes Leaked by Lapsus$ Group
3. Multiple Microsoft Products' Source Code Leaked by Lapsus$ Group
4. Insurance Regulatory Development Authority of India (IRDAI) Compromised by Bully Group
5. 9.8 Million Customer Records from Optus (Singtel) Put on Sale by TA optusdata
6. 16 million Records from the Swachhata Platform (MoHUA) Leaked by TA Leakbase
7. Over 2 Milion Records from MyDeal (Woolfworth) Put on Sale by TA dior
8. 1.2 Million Compromised Payment Cards Data Leaked by BidenCash
9. Uber Breach by TA 'Tea Pot'
10. 400 Million Twitter Scapred Users' Data on Sale by TA Ryushi

EXECUTIVE SUMMARY

THE REPORT ENCAPSULATES THE FOLLOWING **MAJOR FINDINGS** FROM 2022:

Several underground forums were discovered and observed by CRIL in 2022, amongst which BreachForums was highly active in the propagation of data breaches and leaks.

Threat activities impacting entities in Asia, North America, and Latin America were observed to be widely distributed in underground forums.

Threat Actors like **Bjorka, IntelBroker, shadowhacker, kelvinsecurity,** and **GhostSec** were observed to be predominantly active in the underground.

Several ransomware groups with the same moniker as their group names, as well as new threat actors claiming to be ransomware groups, emerged on cybercrime forums in 2022 – a tactic not facilitated earlier by cybercrime forums.

Ransomware attacks on some prominent organizations were directly attributed to threat actors/ Initial Access Brokers (IABs) active on underground forums, indicating their affiliations with nefarious ransomware groups.

Stolen Credentials and Account Compromise (TA006 & T1586) and extraction of Data from Cloud Storage (T1530) were commonly observed vectors in the underground.

The Follina MSDT Vulnerability (CVE-2022-30190), Fortinet Authentication Bypass Vulnerability (CVE-2022-40684), VMware SSTI RCE Vulnerability (CVE-2022-22954), Privileges Escalation (CVE-2022-22960) and Zimbra Collaboration Suite Authentication Bypass Vulnerability CVE-2022-37042, Arbitrary File Upload Vulnerability (CVE-2022-27925) were some of the vulnerabilities that we observed being weaponized by TAs.

Brute Ratel C4, Cobalt Strike, Silver Framework, and Mimikatz were observed being actively marketed tools on cybercrime forums.

Phishing-as-a-Service(PaaS), Ransomware-as-a-Service (RaaS), Bulletproof Hosting, Fast Flux Services, and EV Code Signing services gained a lot of traction in the underground.

We foresee cybercriminals modifying their techniques to mass-market their exploits and data breaches through this new medium.

We anticipate that FinTech, E-commerce, Energy, Telecom, and Semi-Conductor organizations may witness higher threats, in line with the trends observed in 2022.

Threat activities targeting Critical Infrastructure due to mass-exploiting techniques and tools emanating from cybercrime forums are likely to increase.

CYBERCRIME FORUMS – AN EXPANDING ECOSYSTEM

2022 witnessed the seizure of the long-standing cybercrime forum RaidForums in February, which saw mass utilization by threat actors during 2021. A few weeks later, BreachForums was established by the threat actor **pompompurin** and introduced as an alternative to the RaidForums.

The design and aesthetic elements were identical for obvious reasons. The forum attracted nearly 250,000 registrations within nine months of its inception in 2022, and many prolific threat actors from RaidForums migrated to BreachForums.

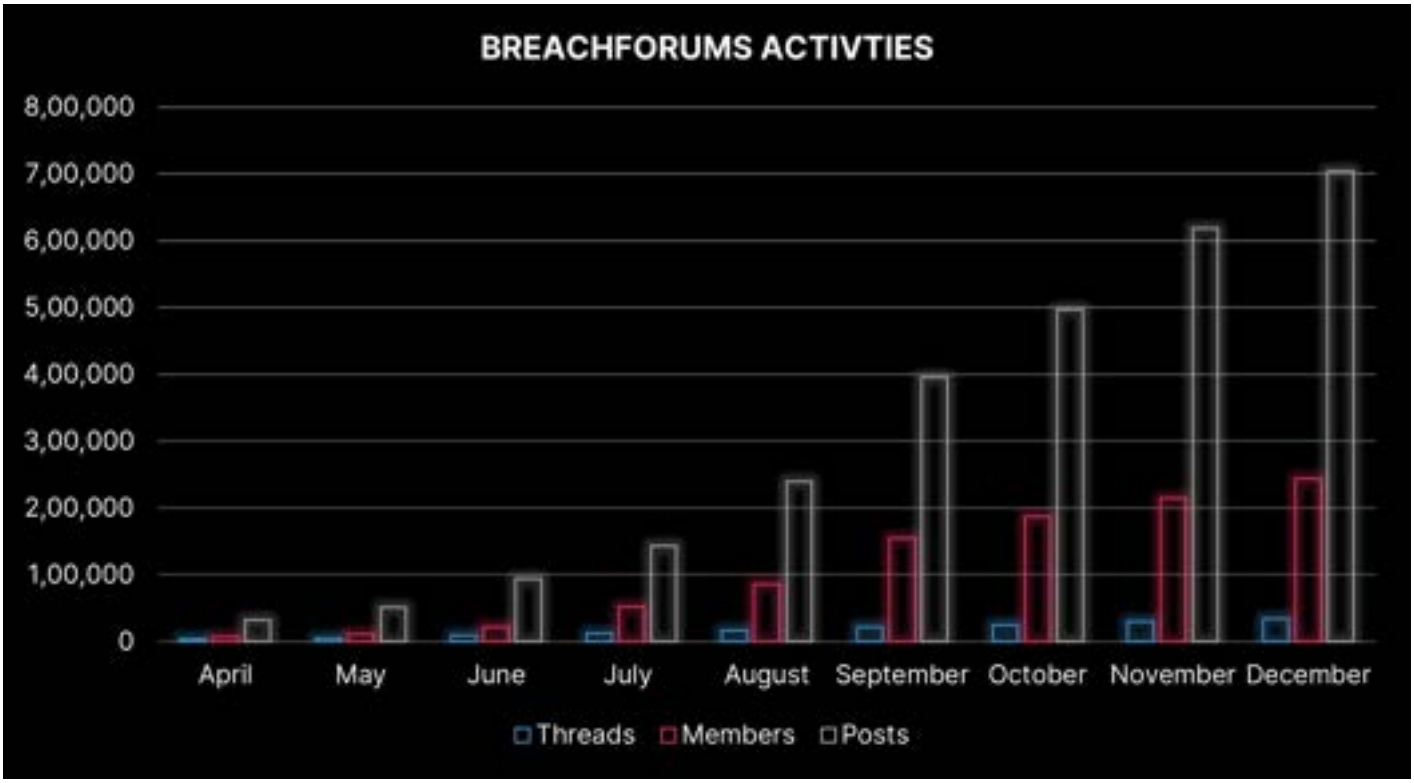


Figure 1: BreachForums Statistics

Throughout the year, threat actors primarily targeted organizations in Brazil, Indonesia, Malaysia, Mexico, and Thailand. This trend initiated with low-level threat activities was intensified by high-level actors and groups such as DESORDEN and Bjorka with an opportunity to monetize these risks. The nations targeted by Threat actors were highly prone to cybersecurity risks.

Bjorka and **LeakBase** offered huge datasets of compromised Personally Identifiable Information (PII) data allegedly stolen from various government and private organizations. At the same time, **DESORDEN** leveraged its capabilities to extort the organizations based on compromised data and then monetize the same on BreachForums in case of a failed extortion attempt.

Apart from the threat actors heavily monetizing compromised data, extortion groups such as **Bully** and **IntelBroker** were observed extending their financial gains through the sale of access and data of victim organizations on BreachForums.

CYBERCRIME FORUMS – AN EXPANDING ECOSYSTEM

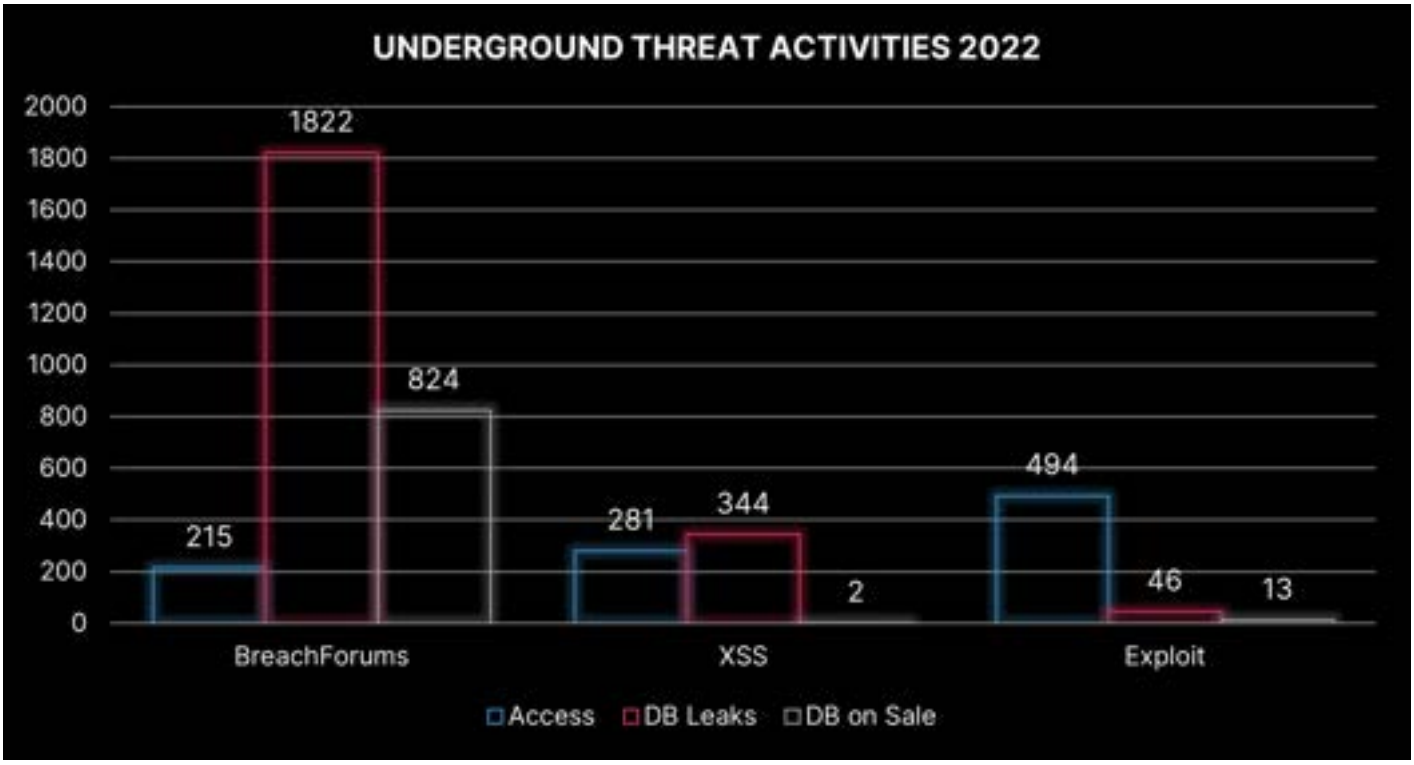


Figure 2: Indicative Statistics of Underground Forum Activities

The Russian cybercrime forums, XSS and Exploit, continued to thrive in 2022 with their sophisticated threat activities ranging from malware development, sale of zero-day exploits, phishing services, sniffer tools, compromised payment card bases, and auction of unauthorized initial accesses.

The prohibition of ransomware affiliate programs and recruitment remained imposed on XSS and Exploit in 2022, but the ransomware operators continued to propagate their operational requirements discreetly.

The historical activities in the underground have brought a drastic shift in threat actors' tendencies and maneuvers to drive financially-motivated operations. The change that started to unfold in 2018 was precisely evident in 2021-2022 via these forums and is an alarming precursor to what we may see in 2023.

Another significant shift observed in TA's tactics on underground forums was the aggressive promotion of data breaches. Evidently, they understood the underlying financial and legal repercussions of such breaches by naming and shaming these entities - a tactic widely adopted by ransomware groups.

Threat actors are now utilizing the forums originally meant for operational discussions as a superior alternative to underground marketplaces.

UNDERGROUND ACTIVITIES AT A GLANCE

CRIL observes and monitors illicit activities from various cybercrime forums and profiles them to present a holistic threat landscape emerging from these forums.

MAJOR CYBER INCIDENTS:

The following infographic depicts major incidents distributed in five regions observed in underground forums through 2022:

	ASIA	ANZ	META	NORTH AMERICA	LATAM
JAN	Malaysia's J&T Delivery Services Data breached	Australian dating website NoStrings Data leak	-	7.5 million records of DatPiff users sold online	TA leaked the Brazil-based Professional services Vintepila database
FEB	Beginning of Ukraine-Russia Cyberwarfare	Australian dating website Matchfinder Data leak	-	US-based Airspan Networks data leak	Mexico state police database leaked
MAR	TA AgainstTheWest initiated Operation Renminbi targeting China	Unauthorized VPN access to New Zealand Steel on sale	3 million users' records of TransUnion South Africa hacked	Okta data breach	Mexican exotic car dealer Iconic-Broker database leaked
APR	Phishing campaigns targeting Indian payment card consumers	Sale of unauthorized access to The Commonwealth Bank of Australia	TA kelvinsecurity leaks a department of the Ministry of Education in Saudi Arabia	FraudWatch International's Client Information leaked	TA Selling Access to Brazilian Military Police and Data from Banco Pan S.A.
MAY	690 million records of Indonesian citizens leaked	200,000 Emails and passwords for Australian Federal police on sale	Embassy of Zimbabwe vulnerability and data on sale	Verizon employees' data leaked	Jamaica police federation Database leak
JUN	105 million users' data of Jatis Mobile exposed	Oxfam Database	Cyberattack on three Iranian steel factories	Database 2 Million visa work applications of OnBlick Inc leaked	TA leaked the Brazil-based energy company CPFL Energia database
JUL	Database of Shanghai National Police (SHGA) leaked	Alleged Access to LMS Energy Pty Ltd. on Auction	Compromise of Bahraini ISP Etisalcom	6 million users' data from US federal agency Centers for Medicare & Medicaid Services (cms.gov) leaked	14.6 Million records from Comisión Federal de Electricidad (Mexico) leaked by TA HolisticKiller
AUG	IndiHome Data Leaked by Bjorka	TA leaked 125,000 emails from the Western Australian Land Information Authority	Emirati company Al Ghurair Iron and Steel database leaked	US-based online food delivery platform DoorDash, Inc data breach	Supreme Court of Justice of Buenos Aires user data on sale

UNDERGROUND ACTIVITIES AT A GLANCE

	ASIA	ANZ	META	NORTH AMERICA	LATAM
SEP	1. 16 Million user records from Swachhata App by MoHUA, India 2. Over 350 Million records of ASKfm & Ask.com data leaked 3. 105 Million Indonesian citizens' data from the KPU server (Indonesia) data leaked 4. 1.3 Billion SIM registration records from KOMINFO, Indonesia, were leaked	Optus Telecom Data Breach	YemekSepeti data on sale	Uber Technologies data breach	Unauthorized access to an unidentified bank based in Costa Rica
OCT	Unauthorized access of India's IT consulting company, Tata Consultancy Services Limited (TCS), and Nuclear Power Corporation of India Limited (NPCIL) on sale	TA dior offers to sell 1.4 million customer records from MyDeal Australia	Unauthorized access to the South African Eskom Hld SOC Ltd. by TA Everest (ransomware operator)	Comcast corporation data breach	Data of 603,000 users of Brazilian MLM company Amigas leaked
NOV	1. 789,446,901 records of Indian voters data leaked 2. Indonesia's COVID-19 contact tracing app, 'PeduliLindungi' data breach 3. 55 Million records of Ftcash data leaked 4. 44 Million records from MyPertamina data leaked	Australian dating website Biaustralia data leak	Saudi Arabia's Smart Link BPO Solutions data leak and HSYS Turkish citizens' health data leaked	Sensitive information about the US Government leaked	Superior Court of Justice Tlaxcala, Mexico data breach
DEC	Indian Railways users' data from RailYatri leaked	Australia-based dental clinic, Dental One data on Sale	Morocco and Algeria's ministries of education data leaked	Infragard users' data leaked	Unauthorized access to Brazilian telecom Algar on sale

UNDERGROUND ACTIVITIES AT A GLANCE

PROLIFIC THREAT ACTORS IN THE UNDERGROUND

GHOSTSEC

- Active Since: June 2022
- Forums: BreachForums
- Activity: Access Broker/ Data Broker

ALL3IN

- Active Since: May 2022
- Forums: BreachForums
- Activity: Data Broker

USDoD

- Alias: NetSec, NetSecOfficial, Scarfac33, ScarFace_ TheOne, Mr. K Smith
- Active Since: November 2020
- Forums: BreachForums, Exploit
- Activity: Access Broker/ Data Broker

KILLIANDOROTHY

- Active Since: July 2022
- Forums: BreachForums
- Activity: Access Broker/ Data Broker

SHADOWHACKER

- Alias: LeakSmart, unvisible, JawiShop
- Active Since: August 2022
- Forums: BreachForums, XSS
- Activity: Access Broker/ Data Broker

KELVINSECURITY

- Alias: teamkelvinsecteam, KelvinSecTeam, Katrine Hacker, Kristina
- Active Since: Beginning of 2018
- Forums: BreachForums,
- Activity: Access Broker/ Data Broker

BJORKA

- Active Since: August 2022
- Forums: BreachForums, XSS, Exploit
- Activity: Data Broker

UNKNOWN (XSS)

- Active Since: July 2022
- Forums: BreachForums, XSS, Exploit
- Activity: Access Broker/ Data Broker

SIGNA

- Active Since: March 2022
- Forums: BreachForums, XSS, Exploit
- Activity: Access Broker/ Data Broker

UNDERGROUND ACTIVITIES AT A GLANCE

RANSOMWARE GROUPS PROLIFERATING IN UNDERGROUND FORUMS

BULLY RANSOMWARE GROUP

The Bully Ransomware Group established their Telegram channel dubbed "Bully Gang" on September 6, 2022, and later joined the cybercrime forum BreachForums under the moniker 'Bully_Support' on September 10, 2022. The group has actively claimed to compromise the targeted organizations, including IRDAI (India), Flintec, Inc. (USA), and Associates Insurance Group Inc. (USA).
Based on these activities, the group's primary modus operandi is as follows:

- Exfiltrate and encrypt data from the targeted organization
- Announce the claims of compromise on their Telegram channel and BreachForums after the alleged refusal to pay the ransom
- Share password-protected sample data
- Propose to sell the stolen data privately

Although the group has been actively posting its claims on the forum, none of the targeted victims have confirmed the attack at this point. The operations of the ransomware group remain uncertain as they have limited activities on the forum and their Telegram channel and are yet to release their own website.

INTELBROKER (ENDURANCE RANSOMWARE GROUP)

TA IntelBroker on BreachForums, proclaimed themselves as the Endurance Ransomware Group. Initially, they were a one-member group that emerged in October 2022 and was even observed hiring affiliates. Ironically, they were also observed seeking help from C# developers to add a list of enhancements in the existing malware (Endurance) developed by the TA.

The TA has allegedly breached several US government organizations and offers Ransomware-as-Service (RaaS) on the forum. Open research results revealed a GitHub page belonging to the TA, which included the source code of the Endurance data wiper malware. The malware was written in C# using the .NET framework. However, the effectiveness of the ransomware remains doubtful.

UNDERGROUND ACTIVITIES AT A GLANCE

DESORDEN GROUP

The TA group DESORDEN gained prominence in late 2021 after a series of alleged high-profile data breaches targeting Asian organizations. They later shared the compromised data on an English-speaking cybercrime forum, RaidForums.

In June 2022, the group, which then had 5-6 members, remerged on BreachForums and started actively posting details on the compromised organizations. Some of the significant targets included Acer (India), Ventura Securities Ltd. (Indonesia), Better Way Co. Ltd. (Thailand), UOB Kay Hian Securities (Malaysia), PT Pertamina (Indonesia), and Centura Hotel Group (Thailand).

According to an article, the TA group described themselves as the former associates of the **ChaosCC** group. They later rebranded themselves as **Desorden group,** which stands for Chaos & Disorder.

They claimed to be financially motivated and specifically targeted supply chain networks to create a larger impact that could potentially affect several parties associated with the targeted organization. The data was sold in case the organizations failed to pay the ransom.

The TA also shared the Yashma Ransomware Builder, besides offering databases on sale. The group allegedly acquired this builder from a private source for testing and reverse engineering.

EVEREST RANSOMWARE GROUP

The threat actor group dubbed **Everest** has been a member of BreachForums since May 2022 and claims to be the owner of the Everest ransomware group. The signature and profile information of the forum handle also mentions the group's leak site and Tox ID.

The group has been selling compromised corporate accesses to the victim organizations announced on the official leak site of the Everest ransomware group. TAs tend to offer unauthorized access to interested buyers upon failing to extort any of their target organizations.

Interestingly, last month, the TA posted a thread inviting forum members for a partnership with the Everest Ransomware group.

RANSOMWARE ATTACKS ATTRIBUTED TO UNDERGROUND ACTIVITY

AUSTRALIAN HEALTHCARE ENTITY RANSOMWARE ATTACK LINKED TO TA RADAR

At the close of 2022, TA RADAR was selling alleged data from Australia-based dental clinic Dental One on BreachForums. The TA is a self-proclaimed ransomware group.

The TAs shared a screenshot of the folder tree of stolen data while mentioning that 500 GB of data from the servers of the Craigieburn-based clinic, consisting of customers' Protected Health Information (PHI), invoices, reports, scans, online forms, important documents, etc. had been compromised.

Dental One operates 5 clinics in Melbourne. CRIL predicted that the extent of the attack may not be limited to Craigieburn clinic and can affect the other four clinics in Melbourne - Lower Templestowe, Epping North, Richmond - Victoria Gardens, and Reservoir.

Our observations were validated as, within a few days, Alphavm, aka Black Cat Ransomware Group, announced that they had targeted Dental One and leaked 6 GB of data. The screenshot shared by the group is similar to what TA RADAR shared on their forum post, but our analysis suggests that the attack impacted all five clinics.

We envisage TA RADAR to be associated with Alphavm through their affiliate program and subscribing to Alphavm's Ransomware-as-a-Service (RaaS). Alternatively, the TA could be advertising the sale of the victim organization's data in cybercrime forums, a trend adopted by some prominent ransomware groups such as Everest and LOCKBIT to apply further pressure and extort their victims for ransoms.

TA 'DATASELL' OFFERED DATA STOLEN FROM INDIANAPOLIS HOUSING AGENCY, POSSIBLY BEHIND THE DOUBLE-EXTORTION ATTACK

On October 6, 2022, several media sources reported that the US-based public housing agency, Indianapolis Housing Agency (IHA), was targeted by a ransomware attack. None of the notorious ransomware and data extortion groups have claimed responsibility for the cyberattack so far.

During a routine threat-hunting exercise, CRIL identified a newly registered Threat Actor (TA) **datasell** on the XSS forum, selling stolen data from unnamed organizations. Investigation revealed that the TA was selling data allegedly belonging to the IHA, which was subject to a ransomware attack.

We continued to investigate the claims and found various artifacts which indicated the threat actor **datasell** possessed data stolen from IHA and could possibly be one of the perpetrators behind this double-extortion attack.

Figure 3: TA datasell's advertisement thread

RANSOMWARE ATTACKS ATTRIBUTED TO UNDERGROUND ACTIVITY

RANSOMWARE ATTACK ON ISGEC; POSSIBLY ATTRIBUTED TO TA BACEPMEH

An Indian online-media publication published an article suggesting ISGEC Heavy Engineering Limited suffered a ransomware attack. An official notice released by ISGEC indicated that on June 7, 2022, unidentified threat actors gained access into their network, encrypted data on their infected servers, and demanded ransom in Bitcoin (BTC).

On April 14, 2022, CRIL had previously identified the Threat Actor (TA) **BACEPMEH**, selling unauthorized access to the Citrix account, allegedly belonging to an undisclosed Indian organization with revenue worth USD 734 Million on the Exploit forum.

Information from multiple sources led us to identify that the allegedly impacted organization was Indian heavy equipment manufacturing company, 'ISGEC Heavy Engineering Limited' (formerly known as Indian Sugar and General Engineering Corporation).

The timeline of events implied that these two incidents were related and that the unauthorized access that the TA **BACEPMEH** was selling might have been leveraged in the ransomware attack mentioned above.

Figure 4: TA BACEPMEH's advertisement on Exploit

RANSOMWARE ATTACKS ATTRIBUTED TO UNDERGROUND ACTIVITY

CYBER-ATTACK BY LOCKBIT AGAINST MEDCOENERGI (INDONESIA) ATTRIBUTED TO INITIAL ACCESS BROKER ON EXPLOIT FORUM

On April 30, 2022, the threat actor **vcc_expert** on Exploit offered to sell unauthorized access to an alleged Indonesia-based Oil and Gas company with revenue worth 1 Billion dollars. Based on the description posted by the TA, it was assumed that the allegedly compromised organization was the Indonesian energy company, 'PT Medco Energi Internasional Tbk'.

On May 2, 2022, **vcc_expert** closed the topic soon after threat actor **913** expressed interest in their offer, indicating the possibility that **913** purchased accesses from vcc_expert. Later, on June 15, 2022, the LockBit Ransomware Group claimed to compromise Medco Energi Internasional.

Threat activities from April 30, 2022, and May 2, 2022, on the Exploit, were followed by a ransomware attack on June 15, 2022. The timeline and TA 913's recent cybercrime activities indicated that the latter could have been an affiliate/associate of the LockBit (2.0) Ransomware Group and may have played a role in the attack against PT Medco Energi Internasional TBK.

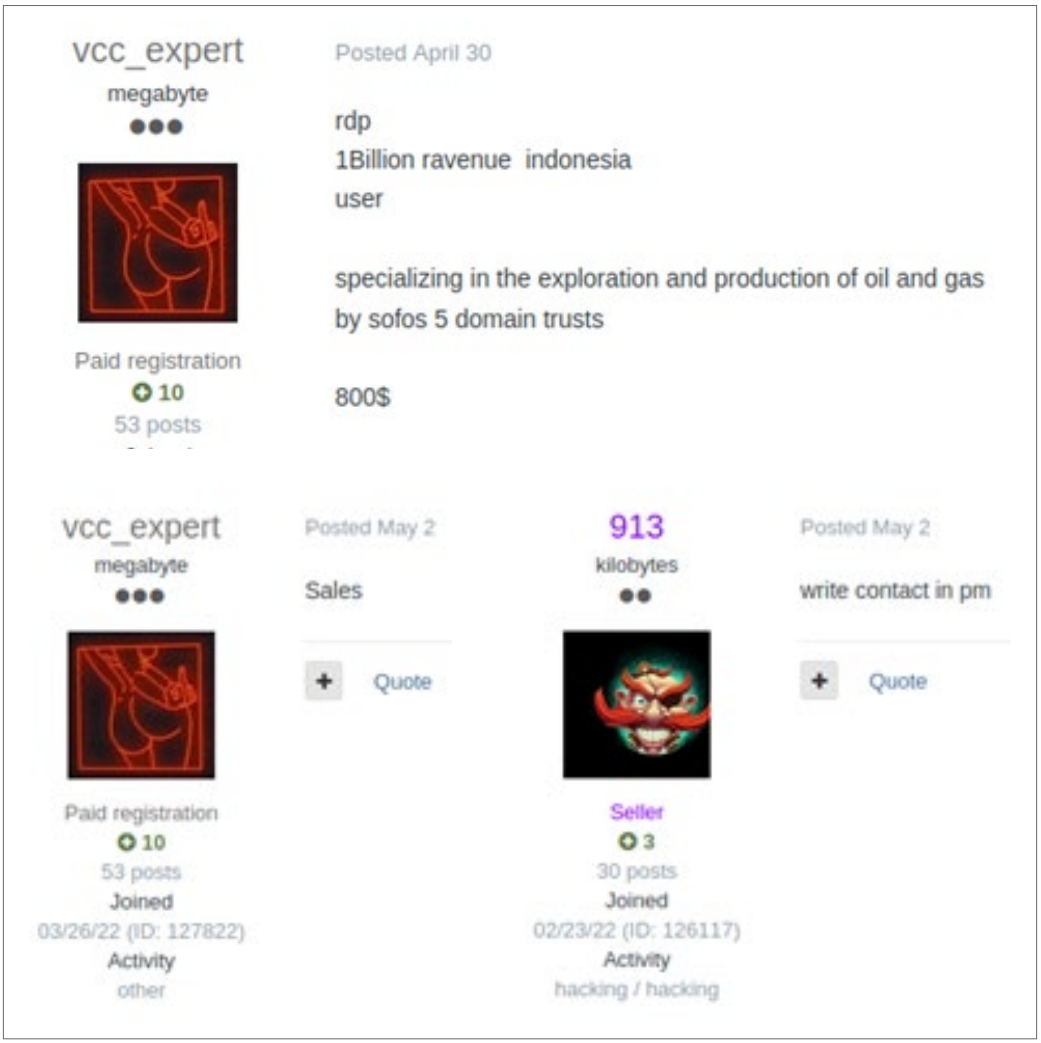
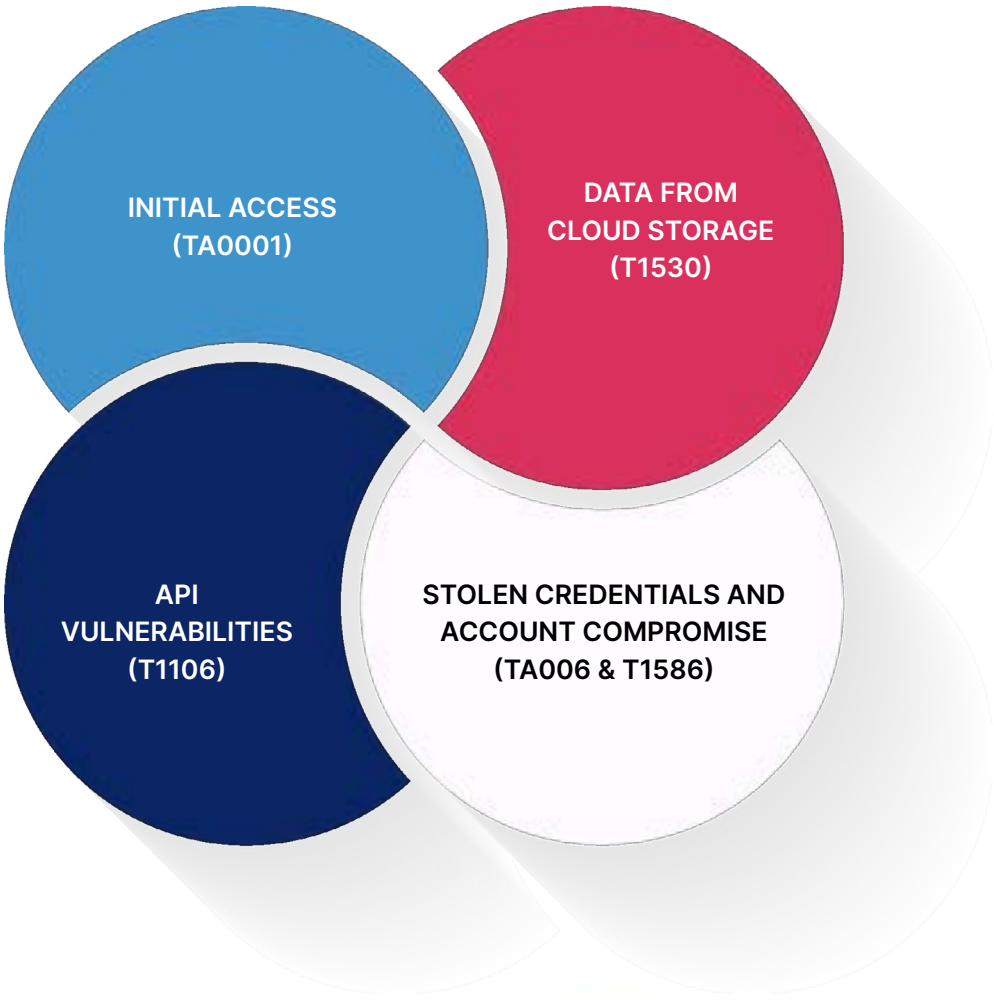


Figure 5: Indonesian company access advertisement thread

MAJOR TACTICS, TECHNIQUES, AND PROCEDURES (TTPs) OBSERVED

THE MOST COMMON TTPs OBSERVED IN THIS YEAR'S MAJOR COMPROMISES, AND BREACHES INCLUDE



MAJOR TACTICS, TECHNIQUES, AND PROCEDURES (TTPs) OBSERVED

INITIAL ACCESS (TA0001)

Initial Access Brokers (IABs) are threat actors who gain unauthorized access to an organization's network by leveraging vulnerabilities or other sources and sell these to buyers who are often associated with the Advanced Persistent Threat (APT) groups, extortion groups, ransomware operators, and individual threat actors.

Figure 6: Olux shop advertising compromised access

Initial Accesses are often offered via Active Directory, Outlook Web Access (OWA) accounts, RDP (Remote Desktop Protocol), VPN Infrastructure, and Citrix, which are described in MITRE TTP **T1133** (remote services). The methods used to obtain these accesses include credential access **(TA0006)** and phishing **(T1566)** to obtain existing valid accounts **(T1078)**.

STOLEN CREDENTIALS AND ACCOUNT COMPROMISE (TA006 & T1586)

Threat actors utilize stolen credentials to the compromised endpoints obtained from information stealer malware as an Initial Access vector. The credentials stolen by the malware from infected devices are stored on a C&C server in the form of logs, usually known as 'stealer logs'.

STEALER LOGS TYPICALLY CONSIST OF THE FOLLOWING:

- User cookies
- Credentials (username, password)
- IP address
- Screenshots
- User-agent Information
- System/device information

MAJOR TACTICS, TECHNIQUES, AND PROCEDURES (TTPs) OBSERVED

The compromised credentials allow TAs to gain unauthorized access and advanced session information - thus enabling authorization into compromised endpoints without raising any flags.

Azorult, Racoon, Redline, and Vidar malware operators advertise their stealer logs on the Russian market, 2easyshop, Genesis, and other popular underground marketplaces. A threat actor looking to target a domain can easily search in the stealer log markets for potentially compromised credentials.

Figure 7: Stealer logs listed on Russianmarket

CASE #1: The threat actors behind the cyber incident at Uber in September 2022 leveraged the cybercrime marketplace to purchase VPN credentials and initiated a full-fledged cyberattack.

CASE #2: On September 23, 2022, CRIL identified that highly-active threat actor LeakBase compromised 16 Million users from the Swachhata Platform. LeakBase likely obtained the admin credentials to the 'Swachh.city' platform from the stealer logs that were readily available in underground marketplaces.

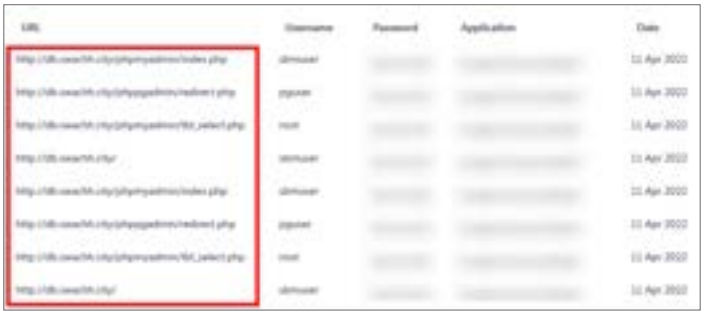


Figure 8: Compromised endpoints identified by Cyble Vision

MAJOR TACTICS, TECHNIQUES, AND PROCEDURES (TTPs) OBSERVED

Dumping databases from exposed administrative panels' backups has been the modus operandi of the TA **LeakBase** in 2022. The TA continued posting large sets of compromised credentials, including 14 million rows of .gov domain credentials. **LeakBase's** other known TTPs included brute forcing and SQL injection again web applications.

Other cases of threat actors leveraging similar TTPs in 2022 are as follows:

- TA, **nativee**, privately offered 117 accesses, impacting government and private entities in Qatar, Saudi Arabia, the US, India, and Thailand. The TA allegedly obtained accesses from a modified Vidar information stealer with an hVNC module.
- TA **hitm50n** offered to sell unauthorized access to an internal administrative panel belonging to the Government of Rajasthan (rajasthan.gov.in), a state in India. Cyble's Threat Intelligence Platform identified 159 SSO credentials belonging to the impacted portal in multiple instances of the stealer malware logs observed since October 1, 2022.
- TA **RADAR** leaked a set of 24 credentials to FTP servers and cPanel of various entities. The credentials appeared to be obtained from compromised endpoints/stealer malware.

DATA FROM CLOUD STORAGE (T1530)

Cybercriminals have predominantly abused internet-scanning services such as Shodan and Binary Edge to navigate vulnerable cloud instances, exposing sensitive information.

Misconfigurations in cloud instances have been a prominent vector behind several breaches in 2022, including:

- An Indonesia-based accounting software startup
- An Indonesia-based digital business platform
- An India-based radio taxi provider. The dataset was offered for sale by a TA on the now-defunct RaidForums in July of 2021. Cyble researchers found and reported exposed cloud storage which posed a risk until June 2022
- An elastic database from an India-based game development company (with over 30 million users)
- An AWS S3 bucket exposing the data of 100,000 students registered to an educational publishing company
- The breach of 1 billion Chinese citizens' data records from Shanghai's national police by TA **ChinaDan** was due to exposed access keys shared by a developer in 2020 on a Chinese development discussion board. The developer shared the endpoint address, ID, and access key

Figure 9: Mishandling of access key on a forum

MAJOR TACTICS, TECHNIQUES, AND PROCEDURES (TTPs) OBSERVED

API VULNERABILITIES (T1106)

TAs have been steadily exploiting unsecured APIs (Application Programming Interfaces). API vulnerabilities were typically chained with IDOR (Insecure Direct Object Reference), where a TA sends multiple requests to the API while only changing an identifier, for example, a UID (User ID), to scrape information.

CASE #1: One of the notable cases leveraging similar TTPs was observed in a data breach at an Australian Telecommunications company, 'Optus', entailing the exposure of 9.8 Million customers' PII data.

TA exfiltrated this PII via API abuse and listed it for sale. 10,200 customers' data was released as sample data, leading to a wave of other cyberattacks impacting MyDeal, MyRewards, Telstra, and Medibank.

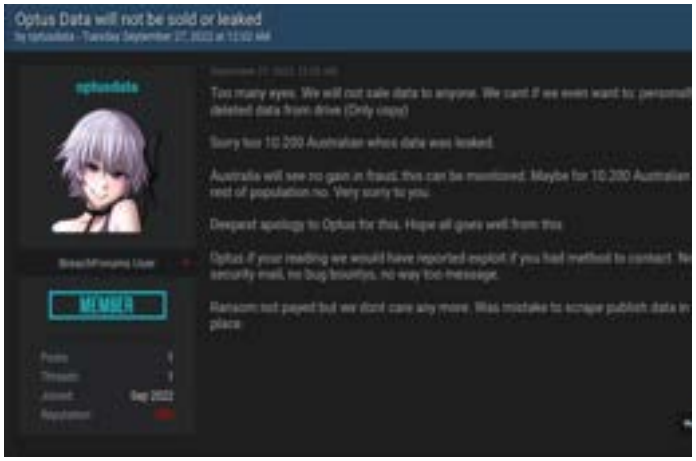


Figure 10: Optus Data on Sale at BreachForums

CASE #2: The data leak of over 30 million Indian passengers' data by **shadowhacker** was linked to a vulnerable API of the RailYatri application to compromise data from the corresponding server.

The data exfiltrated by the TA included invoice records of 30 million users' names, gender, phone number, and other information.

Figure 11: RailYatri database advertisement thread

MAJOR TACTICS, TECHNIQUES, AND PROCEDURES (TTPs) OBSERVED

TARGETING VULNERABLE E-COMMERCE PLATFORMS

E-commerce platforms are one of the most visited websites and store sensitive payment information, which is in high demand in underground marketplaces.

In 2022, we observed that e-commerce platforms based on Magento, WooCommerce, and OpenCart, were heavily targeted. TAs leverage vulnerabilities to obtain unauthorized access in order to install a web shell. The shell could then be leveraged to drops malicious scripts to sniff or steal sensitive debit/payment card data and customer billing details. The sniffed credit card bases are then listed for sale at various credit card shops such as Yale Lodge, BidenCash, and underground forums such as XSS and Exploit.

CASE #1: TA **alexa0907** on the XSS forum claimed to have over ten zero-day exploits targeting vulnerabilities on the WooCommerce platform, including SQL injection and cross-site scripting (XSS). The forum's admin later closed the thread after the vulnerabilities were allegedly sold.

Various CVEs are discussed on the forums along with proofs of concept, such as CVE-2022-24086 - an input validation vulnerability affecting Magento.

Figure 12: alexa0907 selling 0day exploits

CASE #2: Threat actors **Saiwer** and **Evkazoline**, **Germany** offered bulk access to Magento, Joomla, WordPress, and other platforms. TA Saiwer determined the value and tiers of the offered accesses based on the number of orders received at each e-commerce shop. In contrast, TA **haspY** posted the revenue of the compromised shop to advertise their sale.

On the other hand, we observed that TAs **DaffyDuck767** and **estet**, with unauthorized accesses to e-commerce control panels, sought partnerships to place malware for active payment sniffer operation.

Figure 13: TA selling access to Magento, Joomla, WordPress panels

MAJOR TACTICS, TECHNIQUES, AND PROCEDURES (TTPs) OBSERVED

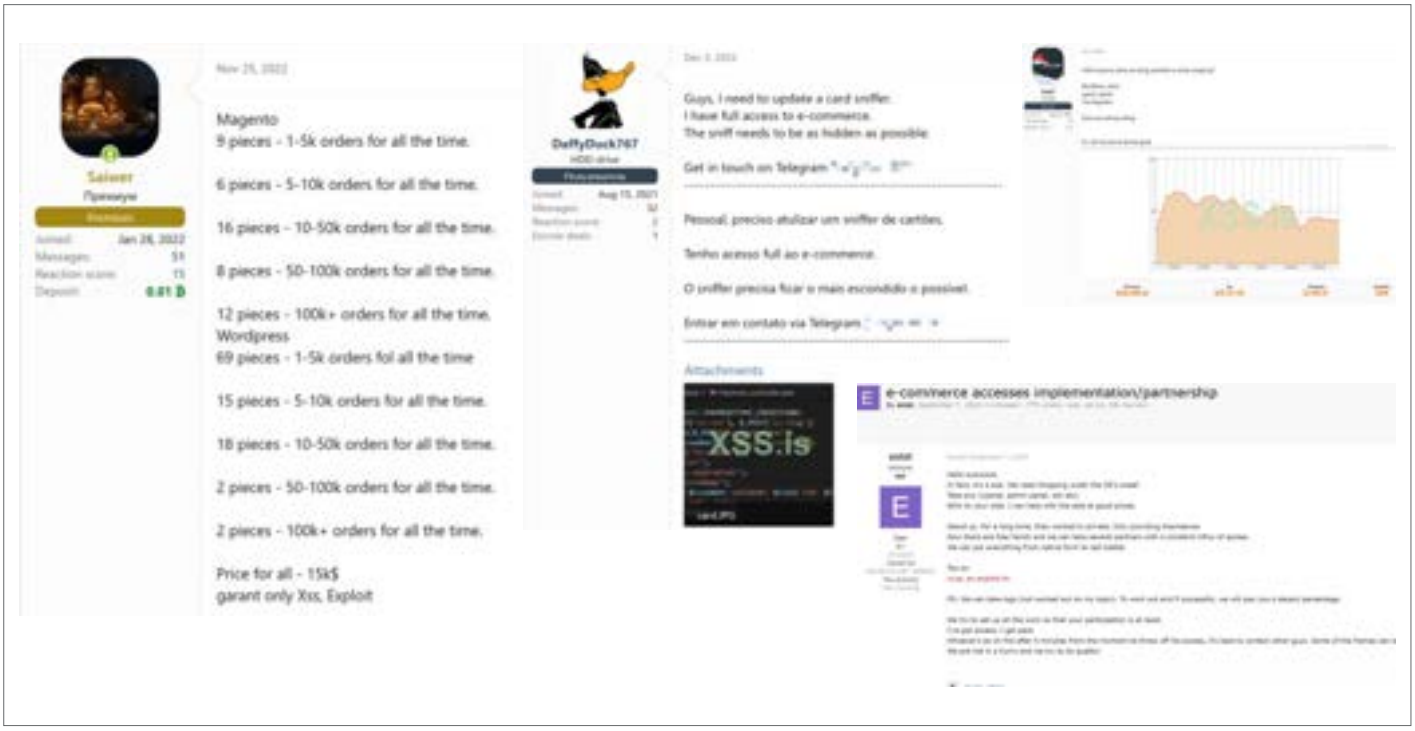


Figure 14: TAs targeting e-commerce panels

CASE #3: TA **mary** advertised access to the admin panel and Zendesk CRM access -allegedly from an Indonesian e-commerce website.

The admin panel allegedly contained over 2 Million customers' information, 9 Million order information, employee information, and the capability to generate promotional codes.

The TA also posted a sample of customer data containing PII such as name, email, mobile number, and city.

Figure 15: Indonesian e-commerce website access advertisement thread

MAJOR TACTICS, TECHNIQUES, AND PROCEDURES (TTPs) OBSERVED

HIGHLY LEVERAGED TOOLS IN CYBERATTACKS

SILVER FRAMEWORK

- Developed in the 'Go' language
- Open-source Command and Control (C&C) system
- Supports asymmetrically-encrypted C&C over DNS, HTTP, HTTPs, and Mutual TLS
- Abused by Russian state-sponsored **APT29**, aka **Cozy Bear**
- A popular alternative to Cobalt Strike

Figure 16: Discussion about Silver Framework

BRUTE RATEL C4

- An adversary Emulation framework to evade detection by EDR and antivirus solutions
- Abused by Russian state-sponsored **APT29**, aka **Cozy Bear**
- Served as a common second-stage payload from botnets such as QAKBOT, IcedID, Emotet, and Bumblebee

Figure 17: Brute Ratel C4 License on Sale

MIMIKATZ

- An open-source tool abused to steal credentials, gain unauthorized access to networks or systems, privilege escalation, or lateral movement within a compromised network
- Used in many ransomware campaigns, including DoppelPaymer, Nefilim, NetWalker, Maze, ProLock, RansomExx and Sodinokibi
- Abused by Iran-based **Agrius** in various supply-chain attacks against Israel and UAE since 2020

Figure 18: TA allegedly dumped credentials to a Spanish Organization using Mimikatz

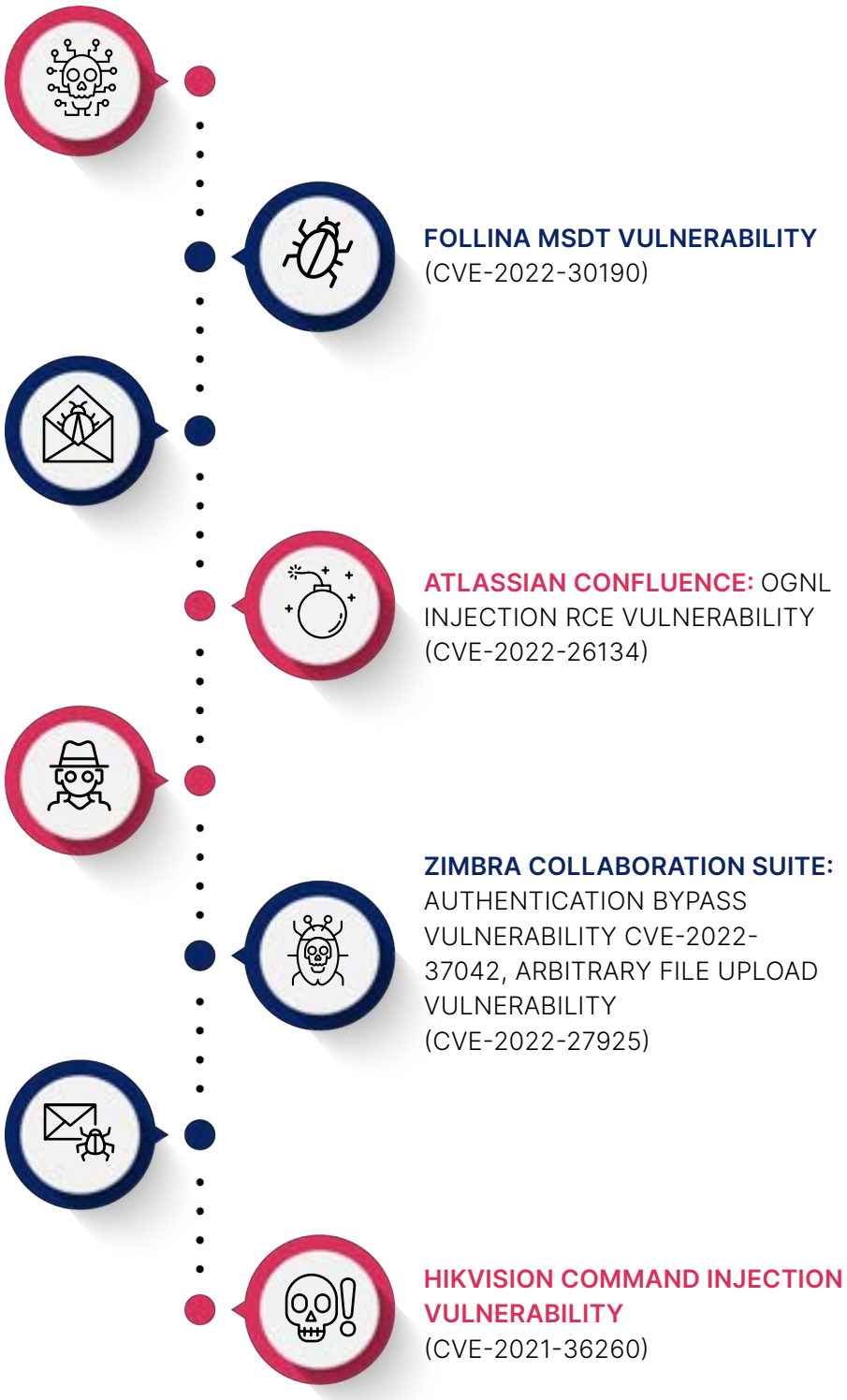
COBALT STRIKE

- A red-teaming tool providing different functionalities, including privilege escalation, implementation of Mimikatz, port scanning, and lateral movement
- Supports C&C and staging over HTTP, HTTPs, DNS, SMB
- Abused in many ransomware campaigns by Clop, Conti, DoppelPaymer, Egregor, Hello (WickrMe), Nefilim, NetWalker, ProLock, RansomExx, Ryuk ransomware groups

Figure 19: COBALT STRIKE on Sale

MOST WEAPONIZED VULNERABILITIES IN THE UNDERGROUND

THREAT ACTORS WERE OBSERVED PROMPTLY WEAPONIZING EXPLOITS AND OFFERING LEAKS FROM VARIOUS PUBLICLY DISCLOSED VULNERABILITIES.



MOST WEAPONIZED VULNERABILITIES IN THE UNDERGROUND

1 PROXYNOTSHELL (CVE-2022-41040, CVE-2022-41082)

During August 2022, researchers at GTSC discovered and later reported to Microsoft certain critical vulnerabilities impacting the Microsoft Exchange Server, known as 'ProxyNotShell'. Similar to its predecessor ProxyShell, ProxyNotShell is also a chainable set of following vulnerabilities that may be exploited to take over Microsoft Exchange email servers:

CVE-2022–41040: A Server-Side Request Forgery (SSRF) vulnerability allowing an authenticated attacker to trigger the second vulnerability, CVE-2022–41082, remotely.

CVE-2022–41082: This vulnerability allows Remote Code Execution (RCE) when PowerShell is accessible to the attacker.

NOTABLE OBSERVATIONS IN UNDERGROUND FORUMS:

On November 12, 2022, TA **SebastianPereiro**, on Exploit, offered to sell Remote Code Execution (RCE) exploit code for the ProxyNotShell vulnerabilities. Another TA, **greedman**, purchased a copy and posted positive feedback.

At the same time, one of the other forum members contested **SebastianPereiro's** offer with a publicly released PoC by GitHub user **testanull** on November 18, 2022.

SebastianPereiro clarified that their exploit differed from the publicly available ones and was designed to target multiple entities.

Figure 20: ProxyNotShell exploits advertisement thread

2 FOLLINA MSDT VULNERABILITY (CVE-2022-30190)

Disclosed in May 2022, the vulnerability CVE-2022-30190 (aka Follina) allows the attacker to abuse the Microsoft Support Diagnostics Utility (msdt.exe) via the ms-msdt, a protocol to download malicious Word documents (or Excel spreadsheets) from the web.

Additionally, there are known techniques to misuse Wget in PowerShell. The attacker can abuse the flaw to remotely execute code with the privileges of the calling application. Various threat actors in underground forums frequently discussed and monetized this vulnerability.

NOTABLE OBSERVATIONS IN UNDERGROUND FORUMS:

Multiple TA, including **darksoftware, aion, 3xp1r3**, and **Windefender** on Exploit and XSS forum, were seen offering an exploit builder to generate an undetectable executable embedded within a document file, targeting CVE-2022-30190.

At the same time, TA **gordsnob** offered loader malware to exploit CVE-2022-30190 via malicious document files.

Figure 21: Follina Vulnerability exploits advertisement threads

MOST WEAPONIZED VULNERABILITIES IN THE UNDERGROUND

3 FORTINET: AUTHENTICATION BYPASS VULNERABILITY (CVE-2022-40684)

Disclosed in September 2022, this vulnerability allows an unauthenticated attacker to perform operations on the administrative interface via specially crafted HTTP or HTTPs requests via authentication bypass using an alternate path or channel [CWE-288] in Fortinet FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0.

NOTABLE OBSERVATIONS IN UNDERGROUND FORUMS:

On November 28, 2022, the TA **darksoftware** on the Exploit forum offered a fully-automated exploit weaponizing CVE-2022-40684 vulnerability for USD 5,000. The TA offered two versions – a Python-based exploit for individual execution and a Ruby-based exploit module compatible for exploitation via the Metasploit Framework.

They also shared thorough instructions for the usage of the exploit. The exploit was allegedly capable of checking vulnerabilities in the targeted hosts. If vulnerable – it could create or delete VPN users, extract VPN credentials, allow SSH posts for external access, and add any public key for attackers to manage the router via SSH.

Similarly, on December 31, 2022, TA **LORD1** offered to sell a private exploit weaponizing CVE-2022-40684 vulnerability.

Figure 22: Fortinet Vulnerability exploits advertisement threads

4 ATLASSIAN CONFLUENCE: OGNL INJECTION RCE VULNERABILITY (CVE-2022-26134)

Disclosed in June 2022, CVE-2022-26134 is a critical unauthenticated, Remote Code Execution vulnerability in the Confluence Server and Confluence Data Center. It is an OGNL (Object-Graph Navigation Language) injection vulnerability affecting the HTTP server.

The exploit comprises an OGNL payload sent via the HTTP request in a URL and can be customized to alter the HTTP Response to print the output of the remotely executed commands. Any HTTP method, whether valid (GET, POST, PUT, etc.) or invalid (such as BALH), seems to provide the desired output.

NOTABLE OBSERVATIONS IN UNDERGROUND FORUMS:

From June 22, 2022, till June 28, 2022, **TA r1z** on XSS offered to sell unauthorized root access to the Confluence Servers of 25 undisclosed US-based organizations allegedly compromised by an RCE vulnerability.

TA **nopiro**, who previously contradicted **r1z's** sale of access, posted various indications suggesting the access were probably obtained by weaponizing the Atlassian Confluence OGNL Injection Vulnerability, CVE-2021-26084.

On September 1, 2022, another TA **EmeliRouse** on XSS, offered unauthorized access to 100 undisclosed Confluence servers with varying privileges for USD 500.

Figure 23: Atlassian Confluence vulnerability exploits advertisement threads

MOST WEAPONIZED VULNERABILITIES IN THE UNDERGROUND

5 VMWARE SSTI RCE VULNERABILITY (CVE-2022-22954) AND PRIVILEGES ESCALATION (CVE-2022-22960)

An advisory released by the CISA on May 18, 2022, stated that the threat actors were actively exploiting a series of unpatched vulnerabilities in various VMware-based applications to gain unauthorized access.

CVE-2022-22954 enabled the threat actors with network access to exploit a server-side template injection resulting in Remote Code Execution (RCE), and CVE-2022-22960 enabled threat actors with local access to escalate privileges due to improper permissions in the support scripts.

The threat actors leveraged CVE-2022-22954 to spread a malicious Dingo J-spy web shell. Both of the vulnerabilities impacted several VMware products, including Workspace ONE Access - versions 21.08.0.1, 21.08.0.0, 20.10.0.1, and 20.10.0.0.

NOTABLE OBSERVATIONS IN UNDERGROUND FORUMS:

On July 20, 2022, TA **nopiro** on Exploit released a list of URLs indicating unauthorized access via web shell to various remote access points for domains hosting VMWare Software-as-a-Service applications.

The remote access points belonged to multiple organizations worldwide. According to **nopiro**, the leaked accesses were originally offered by the TA **r1z**. The post also indicated that the TA nopiro leaked access supposedly after a dispute with r1z, who has been selling access to various multiple organizations worldwide on XSS and Exploit forums.

During our analysis, we found that the impacted remote access points were hosted at the end-point management platform - VMware Workspace ONE. A screenshot from one of the compromised accesses demonstrated that the threat actors downloaded the JSP-based web shell in a directory path "/opt/vmware/horizon/workspace/webapps/SAAS/".

Our in-depth research on forum activity, along with the TTPs mentioned in the CISA advisory, helped us determine that the organizations impacted by the leak of webshell access by nopiro were compromised using the chained exploitation of **CVE-2022-22954** and **CVE-2022-22960** vulnerabilities.

Figure 24: VMware vulnerability exploits advertisement threads

MOST WEAPONIZED VULNERABILITIES IN THE UNDERGROUND

6 ZIMBRA COLLABORATION SUITE: AUTHENTICATION BYPASS VULNERABILITY CVE-2022-37042, ARBITRARY FILE UPLOAD VULNERABILITY (CVE-2022-27925)

Disclosed in August 2022, these two high-severity vulnerabilities impacted Zimbra Collaboration Suite (ZCS). CVE-2022-37042 and CVE-2022-27925 can be chained together to bypass authentication, allowing unauthenticated remote code execution on the affected email servers.

CVE-2022-27925 is a flaw in the mboximport functionality of ZCS, which is used to receive a ZIP archive and extract files from it. An authenticated user can abuse this flaw by uploading an arbitrary file to the system, resulting in directory traversal.

CVE-2022-37042: This authentication bypass flaw affects ZCS releases 8.8.15 and 9.0, allowing an unauthenticated malicious actor access to a vulnerable ZCS instance.

NOTABLE OBSERVATIONS IN UNDERGROUND FORUMS:

On August 26, 2022, TA **Aels**, on Exploit, auctioned web shell access to multiple servers operating on Zimbra Collaboration Suite (ZCS).

In the advertisement thread, **Aels** shared a list alleging access to over 100,000 compromised mailboxes from over 2,700 domains hosted on 758 Zimbra-based email servers allegedly vulnerable to the authentication bypass Remote Code Execution (RCE) vulnerability (CVE-2022-37042).

According to the TA, the web shell provided full control with Zimbra user privileges, and the access was allegedly persistent, even after the servers were patched.

The impacted mailboxes purportedly belonged to payment gateways, web hosting sites, municipalities, state departments, and hospitals predominantly from Asia but also in the US and Europe.

Many TAs were compromising LEAs' (Law Enforcement Agencies') mail servers and creating new email accounts to sell for Emergency Data Requests (EDR). **dior**, a TA on BreachForums, frequently exploited this vulnerability.

Figure 25: Zimbra vulnerability exploits advertisement thread

Figure 26: TA selling Indonesian Police webmail exploited by Zimbra vulnerability

MOST WEAPONIZED VULNERABILITIES IN THE UNDERGROUND

7 ATLASSIAN BITBUCKET COMMAND INJECTION (CVE-2022-36804)

Disclosed in August 2022, CVE-2022-36804 is a command injection vulnerability affecting multiple API endpoints of the Bitbucket Server and Data Center. Using this vulnerability, attackers with access to either a public repository or read permissions to a private Bitbucket repository can execute arbitrary code by sending a malicious HTTP request.

NOTABLE OBSERVATIONS IN UNDERGROUND FORUMS:

TA **onlinechamp** and TA **LORD1** on Exploit offered to sell exploits weaponizing CVE-2022-36804.

Figure 27: Atlassian vulnerability exploits advertisement threads

8 HIKVISION COMMAND INJECTION VULNERABILITY (CVE-2021-36260)

Disclosed in September 2022, CVE-2021-36260 is a command injection vulnerability in the web server of the Hikvision product. An attacker only needs access to HTTP(s) server port (typically 80/443). Due to insufficient input validation, attackers can exploit the vulnerability to launch a command injection attack by sending some messages with malicious commands.

NOTABLE OBSERVATIONS IN UNDERGROUND FORUMS:

We observed a few instances on BreachForums, where some threat actors aggressively targeted Hikvision-based IoT products. **TA maraud3r** consistently leaked Hikvision camera devices information allegedly prone to Command Injection Vulnerability CVE-2021-36260. While TA **assfinder** offered to sell complete reconnaissance information on 1,400 Hikvision camera hosts.

Figure 28: Hikvision's vulnerability exploits advertisement threads

MOST WEAPONIZED VULNERABILITIES IN THE UNDERGROUND

VULNERABILITIES POTENTIALLY WEAPONIZABLE FOR MASS-SCALE ATTACKS IN 2023

CVE-2022-44698

Disclosed in December 2022, CVE-2022-44698 is a security feature-bypass vulnerability in Windows SmartScreen, a feature built into Windows that works with its Mark of the Web (MOTW) functionality that flags files downloaded from the internet.

CVE-2022-27518

Disclosed in December 2022, CVE-2022-27518 is a vulnerability that allows an unauthenticated remote attacker to perform arbitrary code execution on the appliance. By targeting vulnerable instances of Citrix ADC, attackers can exploit this vulnerability to bypass authentication controls and obtain access to targeted organizations.

CVE-2022-42475

Disclosed in December 2022, CVE-2022-42475 is a heap-based buffer overflow in several versions of FortiOS that received a CVSSv3 score of 9.3. This Vulnerability allows an unauthenticated, remote attacker to execute arbitrary code or commands on devices running vulnerable versions of FortiOS via specifically crafted requests leading to Remote Code Execution.

CVE-2022-32548

Disclosed around July 2022, CVE-2022-32548 affects multiple DrayTek router models and allows an attack without user interaction if the device's management interface is configured to be accessible via the Internet. In addition, a one-click attack can also be performed inside the LAN in the default configuration of the device. The attack can lead to a complete compromise of the device, leading to complete network access which can be used to get unauthorized access to internal resources.

ACTIVELY SOUGHT MALICIOUS SERVICES IN THE UNDERGROUND

ACTIVELY SOUGHT MALICIOUS SERVICES IN THE UNDERGROUND

PHISHING-AS-A-SERVICE

Phishing-as-a-Service (PaaS) has been quite prevalent, and their sales continue to thrive in underground forums in 2022 as well. PaaS provides threat actors with a convenient platform to develop, customize, deploy and manage live phishing websites.

The ideal targets of phishing services are users of online banking services, e-commerce websites, cryptocurrency exchanges, online streaming services, web hosting services, and major email services such as Google, Microsoft Outlook, Microsoft Office 365, Yahoo, Proton mail, and iCloud.

THE NOTABLE PHISHING-AS-A-SERVICE OBSERVED IN 2022 ARE AS FOLLOWS:

1. One of the most popular and sophisticated Phishing-as-a-Service, dubbed **EvilProxy**, has been operating on the Exploit forum since August 2020 and continues to provide enhancements, updates, and support for their malicious services via the Exploit forum and internet messaging channels.

   EvilProxy's operations are based on the implementation of reverse proxy, which lets it simultaneously interact with a genuine web page to fetch legitimate information and display it on the phishing panel as expected on a genuine one.

Figure 29: EvilProxy advertisement on Exploit

During its execution, it steals valid session information to bypass the Multi-Factor Authentication (MFA) mechanism during the login operation. The notable features of **EvilProxy** include the following:

- An algorithm to detect and blocks bots and virtualization software
- Manage traffic based on visitors on the phishing and landing pages
- Proxy management for geo-targeted campaigns
- The ability to capture advanced session information and MFA Bypass
- Integration of Telegram and Discord bots for notifications

ACTIVELY SOUGHT MALICIOUS SERVICES IN THE UNDERGROUND

2. The TA **kalashnikov** offers a similar PaaS that has been popular in underground forums since December 2019.

   kalashnikov offers phishing panels targeting American Express, First Tech Federal Credit Union and, Australia-based Suncorp, ANZ Bank, & Commonwealth Bank for USD100 – USD400.

   The TA is a highly reputed vendor of Phishing-as-a-Service and has received positive feedback for their services.

Figure 30: PaaS advertisement by Kalashnikov

3. On April 16, 2022, TA **MertvyeDushi**, offered the source code for Man-in-the-Middle (MitM) technique-based phishing kits. The TA implemented a modified open-source phishing toolkit, 'evilginx2', combined with the reverse HTTP proxy tools 'Modlishka' and 'Muraena' to capture credentials and session information.

   Later, the TA added reverse proxy tool modules for several US-based organizations, including Citibank, Chase, Citizens, U.S. Bank, Huntington, Wells Fargo, and TD Bank.

   MertvyeDushi stated that their phishing kit codes were leaked. However, they will continue to develop more source codes.

   Other prolific threat actors involved in offering phishing services during 2022 were **EasyPhish, eyegod,baggin.bilbo, nakedpages, 50c,** and **NextGen.**

Figure 31: MITM Phishing Kits

ACTIVELY SOUGHT MALICIOUS SERVICES IN THE UNDERGROUND

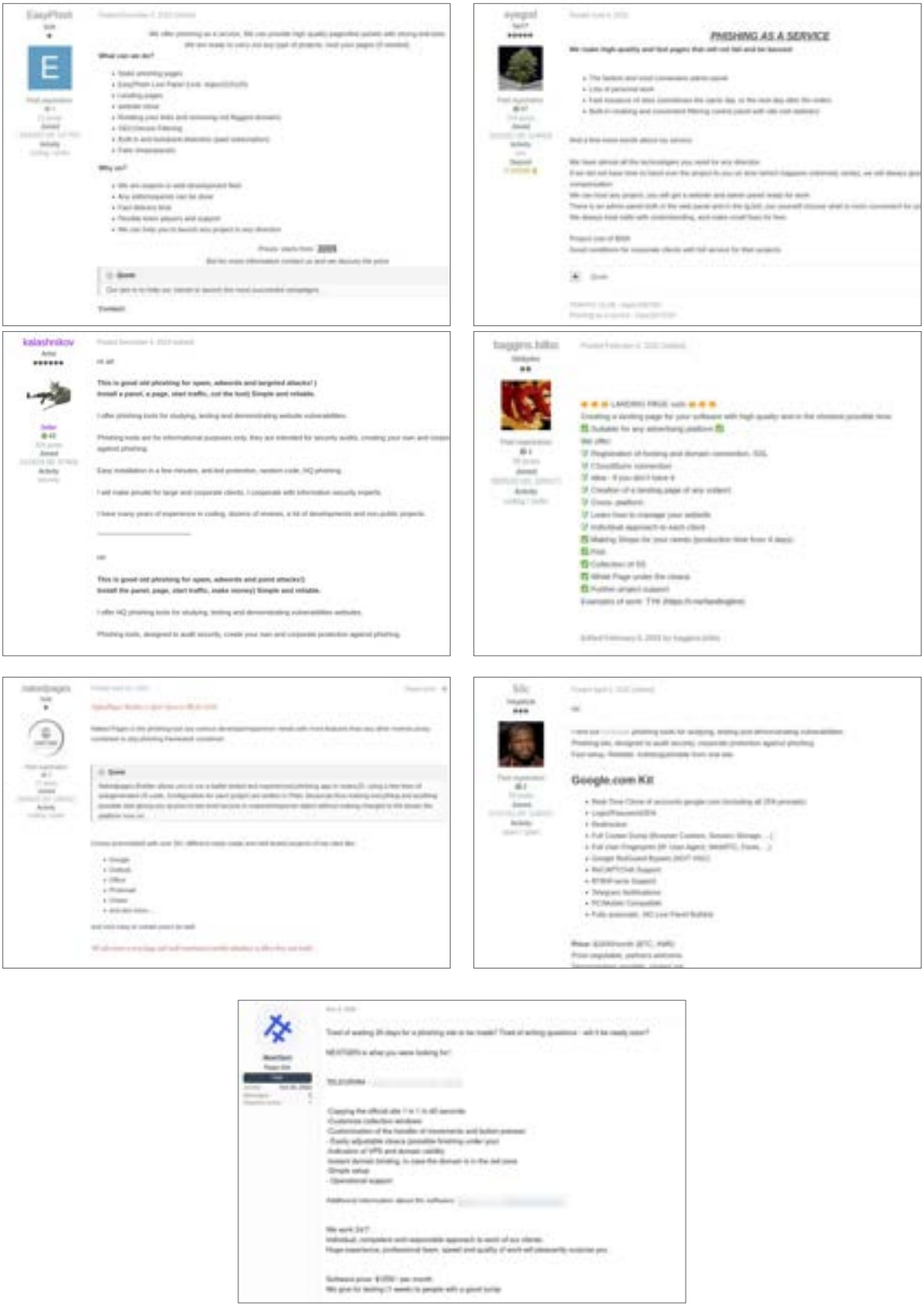


Figure 32: PaaS advertised on Exploit and XSS forums in 2022

ACTIVELY SOUGHT MALICIOUS SERVICES IN THE UNDERGROUND

RANSOMWARE-AS-A-SERVICE

Affiliate programs and services in underground forums are among the most prominent parts of the organized cybercrime ecosystem. 'Ransom-as-a-Service' (RaaS), often called 'Ransomware Affiliate Program', is a cybercrime business model where any threat actor or group can subscribe to a ready-made infrastructure and ransomware kits to spread the malicious infection.

The subscribers or affiliates of the program get various features, including a comprehensive control panel for tracking victims, ransom payments, and a dedicated communication line to extort their victims hosted on a Tor-based web panel.

The majority of ransomware affiliate programs were advertised and propagated via Russian underground forums. However, RaaS operators had to put a stop to their affiliate programs and collaboration efforts due to restrictions imposed by the administrators of major underground forums such as Exploit and XSS in May 2021 to avoid law enforcement actions, supposedly after a ransomware attack against a major American energy company that led to the declaration of an emergency in the state.

RaaS operators remained active on the forums in 2022 but were discreet about their affiliate programs. Many forum members who were known RaaS operators posted advertisements under the guise of carefully chosen words to avoid a ban.

Soon after the announcement on Exploit and XSS, most RaaS operators started listing their affiliate programs and recruitment notices on the Russian language forum RAMP. But, in 2022, we observed a decrease in the RaaS-related activity on RAMP due to alleged links between the owner of the RAMP forum and law enforcement.

The RaaS operators who continued to list their affiliate offers on RAMP in 2022 include - **RTM (RTM Team)**, **fog** (Nevada Ransomware), **ransom** (AlphaV-ng aka Blackcat Ransomware), **MNSTR** (Monster Ransomware), and misteryghost (Luna Ransomware).

One of the notable RaaS operators, **AvosLocker**, advertised their RaaS on the RAMP forum until June 17, 2022, but has since discontinued their ransomware operations on RAMP.

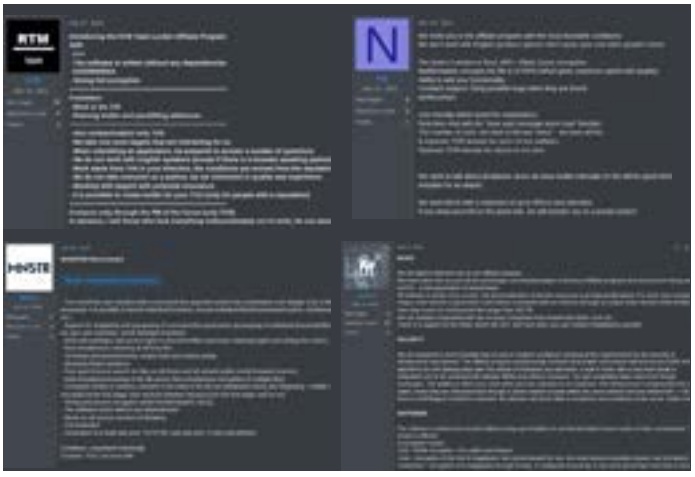


Figure 33: RaaS Advertisements on the RAMP forum

ACTIVELY SOUGHT MALICIOUS SERVICES IN THE UNDERGROUND

BULLETPROOF HOSTING AND FAST FLUX SERVICES

Bulletproof Hosting (BPH), often termed a safe haven for cybercrime groups and criminal syndicates, are the services with their infrastructure in offshore locations or regions lacking authoritarian control or a country that does not abide by international regulations. It offers privacy and resilience from formal complaints from any government or international legal authorities.

BPH services can therefore allow threat actors to host malicious Command-and-Control infrastructure, fraudulent infrastructure, illicit drug marketplaces, terror group-operated websites, cybercrime forums, and websites posting explicit content, which is usually restricted by legitimate commercial hosting services.

On the other hand, fast flux services have become equally popular on underground forums. Fast flux services abuse a pool of compromised hosts or machines in a botnet to rotate the IP addresses of a malicious Command-and-Control (C&C) domain at faster intervals. This masks the original IP address of the C&C and can evade detection.

In order to provide a stable, fast flux network, the Authoritative Nameserver, which is used for name resolution of the malicious C&C domains, is hosted on a bulletproof infrastructure.

The most prolific bulletproof hosting and fast flux network services providers, **Yalishanda** (established 2015), **Ccweb** (established 2010), **Quahost** (established 2013), **BQHOST** (established 2015), and **big.T** (established 2017), continued their operations through 2022.

Figure 34: BPH and Fast Flux services advertised on Underground Forums

ACTIVELY SOUGHT MALICIOUS SERVICES IN THE UNDERGROUND

EV CODE SIGNING SERVICES

Threat actors in underground forums are seen discussing and seeking methods to avoid the detection of their malware without raising flags in a targeted network, safeguarded by sophisticated endpoint security software.

The Extended Validation (EV) code signing certificates are one of the known-yet-sophisticated techniques that have been widely abused in attack campaigns to sign executable files and applications to impersonate their distribution from an authorized publisher, thus evading standard security mechanisms. The absolute demand continued to flourish the code signing services as one of the most sought and expensive malicious service markets in underground forums.

Most prominent techniques to obtain EV Code signing certificates are as follows:

- Stealing EV Certificates from compromised organizations – Short-term business model
- Insider trade of EV Certificates – Semi-scalable and potentially sustainable business
- Anonymous purchase of EV Certificates via a shell corporation posing as a genuine software company - Scalable and sustainable business

We observed various threat actors that claimed to obtain EV code certificates from major certificate authorities such as SSL.com, DigiCert, GlobalSign, Certum, and Comodo.

The EV code signing certificates were advertised for a price anywhere from USD 2,000 to USD 5,000 per code sign. The major sellers were **lopiu** from the Exploit forum and **RastaFarEye, HibanaVelox, unlman,** and **eyesonme** on the XSS forum.

Figure 35: EV Code Signing Services Advertised on the XSS forum

EMERGING THREAT PREDICTIONS FOR 2023

During 2022, we observed threat actors, ransomware operators, developers, and extortion groups expanding their reach to cybercrime forums and Telegram to extort the victims and build their brands. The operators would announce a breach with samples, extorting the victims, before either listing the data for sale or leaking it. We foresee that this shift will continue over time, particularly as ransomware groups look for additional sources of income.

Similarly, malware developers, fraudsters, and hackers will continue to operate on clearnet e-shopping platforms, online advertisements, and the popular voice chat application Discord. Discord has taken down over 55 million accounts and 68,000 servers in the first half of 2022 alone. However, until legislation is implemented to hold e-commerce and social media platforms accountable for users' actions, we will continue to see TAs exploiting these platforms for illicit purposes.

Legislation against cybercrime has been implemented in Indonesia, and amendments to existing legislation are pending in Australia. We foresee governments stepping up to stricter cybersecurity regulations and policies to safeguard their national and economic interests. This development will more likely be observed in smaller nations with greater investments in cybersecurity.

TAs may utilize AI/ML (e.g., ChatGPT) to develop malicious code or finetune shortcomings in their existing code. Lower-skilled malicious actors may begin malware development as well.

We expect that with new cybercrime forums and marketplaces emerging, traditional threat actors may steer clear of present forums to more private forums or mediums to monetize their exploits and/or collaborate with ransomware groups.

ICS (Industrial Control Systems) and SCADA (Supervisory Control and Data Acquisition) were targeted, along with critical infrastructure such as nuclear facilities. Our research predicts more attacks on ICS as part of cyberwarfare and nations' state actors' activities.

REFERENCES

https://tomforb.es/infosys-leaked-fulladminaccess-aws-keys-on-pypi-for-over-a-year/

https://www.theregister.com/2022/12/20/mcgraw_hills_s3_buckets_exposed/

https://www.hcamag.com/au/news/general/optus-hack-exposes-australias-lagging-cyber-law-framework/423724

DISCLAIMER

This document is created to share our findings and research with the broader cybersecurity community from an academic and knowledge-sharing standpoint. It is in no way an endorsement of the activities described in the report or to cause any type of damage to the affected parties. The data points and observations are indication of events observed for the period discussed in the report and publication time. Cyble is not liable for any action(s) taken based on these findings and any ensuing consequences.

FREE EXTERNAL THREAT PROFILE REPORT!

WE GO INTO THE DARKWEB SO YOU ARE NO LONGER IN THE DARK!

- Is your business under threat?
- What are your critical vulnerabilities?
- Blind spots in your digital risk footprint?
- Are your credentials exposed in the darkweb?
- How immune are you to targeted ransomware attacks?
- Are cybercriminals leveraging your compromised endpoints and misconfigurations?

KNOW ALL THIS AND MORE!

GET YOUR ORGANIZATION'S EXTERNAL THREAT PROFILE REPORT

GENERATE FREE REPORT

- CUSTOMIZED SECURITY ASSESSMENT
- TAILORED AND CONTEXTUAL BRIEFING
- UNIQUE RISK SCORE ON SECURITY POSTURE
- EARLY-WARNING ACTIONABLE INTELLIGENCE

ABOUT US

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organizations with real-time visibility to their digital risk footprint. Backed by Y Combinator as part of the 2022 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Start-ups to Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence.
To learn more about Cyble, visit www.cyble.com