An in-depth look at Black Basta's TTPs

intel471.com/blog/an-in-depth-look-at-black-bastas-ttps

The **Black Basta** group ranks as one of the top 10 most prolific and destructive ransomware-as-a-service (RaaS) gangs of all time. In December 2023, a cryptocurrency analysis firm and an insurance company estimated the group had collected at least US $107 million in ransoms. This staggering sum was due to **Black Basta** leveraging myriad attack vectors to compromise networks. This insight comes from a recent leak of 197,000 Matrix chat messages covering about a year of the group's private communications from 2023 to 2024. The chat leaks indicate **Black Basta** attempted to target or attacked at least 583 entities at different times. About 60% of the targeted entities were based in the U.S. The five most-impacted industries in descending order were law services and consulting; industrial products and services; information technology (IT) or technology consulting; engineering and construction; and retail, wholesale and distribution.

The group conducted sophisticated reconnaissance, used private botnets to distribute bespoke malware, leveraged stolen credentials, conducted brute-force attacks, administered phishing campaigns, exploited software vulnerabilities and directly social engineered victims over the phone. Although **Black Basta** developed many of its tools in house, it outsourced several services and tools of other cybercriminal vendors. This combined approach meant the group gained a steady stream of potential victims to turn over to its malicious penetration testers. Those attackers then sought to move laterally, steal data and deploy file-encrypting ransomware if the conditions allowed. Based on a selection of the leaked chats, **Black Basta's** most fruitful years were in 2022 and 2023, and there are indications that by 2024 an increasing number of compromised organizations were in positions to decline to pay ransoms. As of February 2025, the gang appears to have ceased activity, with only eight compromised organizations listed on its data leak blog in January 2025.

Intel 471 analysts have derived deep insight from the leaked chat messages into how **Black Basta** targeted its victims. This insight can be used by organizations to strengthen their cyber resilience and put in place better defensive controls. Despite **Black Basta's** inactivity, these threat actors are likely to regroup or continue their activities by either rebranding or joining other ransomware actors. This means the group's tactics, techniques and procedures (TTPs) discussed below are still relevant for defenders, as some are used by other ransomware actors.

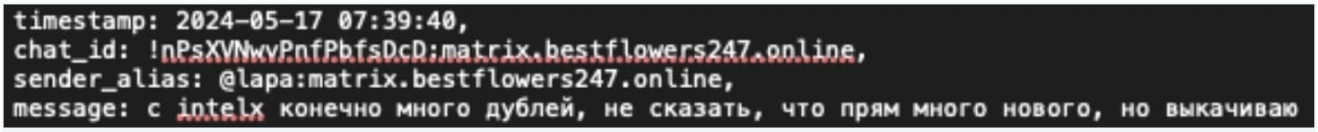
Reconnaissance

The **Black Basta** group used a wide range of free and paid open source and business intelligence services and tools to gather information on potential targets. These include:

— Gathering information from RocketReach and ZoomInfo about potential targets' employees, revenues, etc.

— Leveraging the Censys, FOFA and Shodan search engines to find exposed and/or potentially vulnerable internet-facing hosts or systems.

— Operating a paid account or accounts at the Intelligence X aka IntelX search engine and data archive platform to collect leaked user credentials and use them for brute-forcing attacks as shown in the message below:



The image depicts a screenshot of the **Black Basta** group member **lapa** claiming to use the IntelX service for brute-forcing May 17, 2024 (translated from Russian):

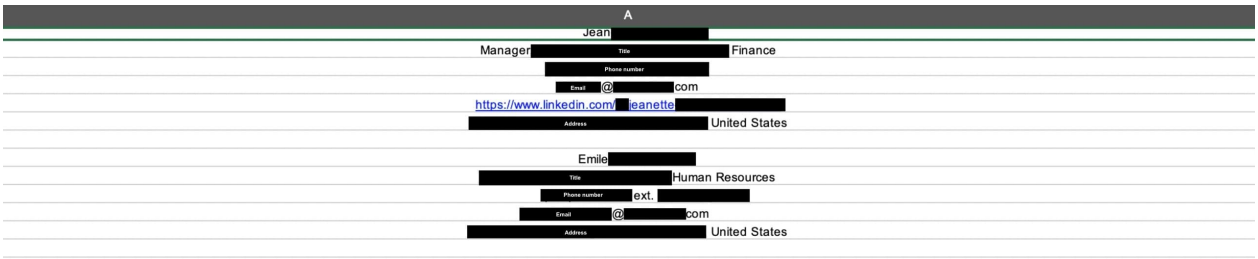
—

@lapa: IntelX has a lot of repeating and old credentials, but I'm still dumping databases from there

—

— Using a private dataset or datasets to enrich information about companies' employees for phishing attacks.

The group methodically collected information about its potential targets. Information about specific employees was often recorded in Google Sheets for distribution to a social-engineering team, who would then call victims to try and gain initial access (more information on that technique will follow). Some of the spreadsheets were still live when the chat logs were released. Intel 471 analysts counted more than 5,000 employees from many organizations who worked in departments such as accounting, marketing, sales, customer service, financial and human resources (HR).



An example of how **Black Basta** listed potential phishing targets in Google Sheets.

Initial access

The group used a variety of methods to gain initial access to victims' networks and deploy malware, which included:

— Employing brute-forcing techniques to collect valid access credentials for remote desktop protocol (RDP) and virtual network computing (VNC) accounts of potential victims. The actors harvested login and password combinations from public information-stealing

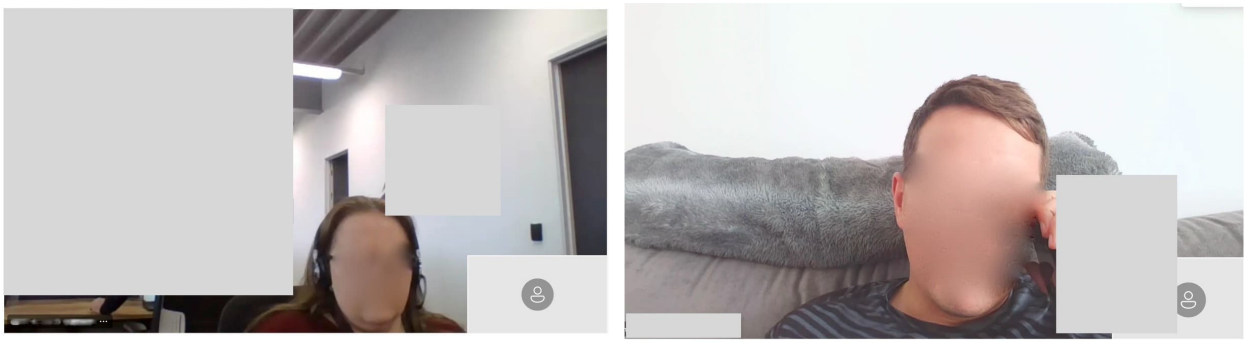
(infostealer) malware logs, IntelX and other sources.

— Using several infostealer malware strains to harvest compromised access credentials. The chat logs contained discussions regarding the Lumma aka LummaC2, MetaStealer, Stealc and Vidar products.

— Partnering with initial access brokers (IABs) on underground forums to purchase compromised access credentials. IABs specialize in selling access to systems, which can involve the sale of credentials or knowledge of vulnerabilities. Groupmembers who went by the personas **usernameugway**, **usernameboy** and **usernamehunter**, among others, were responsible for such operations.

— Using phishing attacks in conjunction with social engineering for initial compromise. The group operated an in-house team of callers that impersonated technical support and conducted telephone-oriented attack delivery (TOAD) campaigns. Attackers abused legitimate remote monitoring and management (RMM) tools, such as AnyDesk, Quick Assist and TeamViewer, to establish a foothold in organizations.

In one scenario, an employee would be targeted in a spam attack that would fill the person's inbox. Then, someone from **Black Basta** would call the person and — reading from a predrafted script — impersonate an IT support member from the victim's organization. The attacker would offer to install antispam software on the user's machine, but in order to do that, the victim needed to install remote access software.



The group captured web camera images of some of its voice phishing (vishing) targets, some of which were included in the chats.

After the victim installed the software, **Black Basta** would contact one of its malicious penetration testers, who would then try to install additional malware to enable persistent access. The pentester would provide a code the victim was supposed to enter on the computer, allowing the pentester to establish another foothold. The leaked chat messages did not reveal what malware was used to obtain persistent access. However, one member claimed to run a batch (.bat) file that prompted the employee to enter credentials for the corporate virtual private network (VPN) portal. These credentials would then allow **Black Basta** actors to access the domain network, advancing the data exfiltration and ransomware attack by one more step.

— Using phishing pages mimicking the Citrix, Cisco, Fortinet, GlobalProtect and SonicWall VPN services as well as Microsoft Remote Desktop Web (RDWeb) accounts. These phishing attacks sought to exploit the dependence on network edge devices and remote access tools. The success of a phishing attack depends on how well the lure is created. A **Black Basta** threat actor going by the name **tinker** had a special talent for writing phishing emails and social engineering content, such as scripts for cold calls made to potential victims, as well as ransom demands.

The leaked chats contain many conversations between **tinker** and **usernamegg** aka **GG**, **tramp**, the leader of the **Black Basta** gang whose real-world identity is likely Oleg Nefedov (see our blog here). In one example, **tramp** tasked **tinker** with creating a phishing email for a campaign that targeted users of FortiClient VPN software. The phishing email contained a fake security notice with a malicious link to a fake corporate login portal. In another example in May 2024, **tramp** called on **tinker** to draft a phishing scenario to target corporate employees that involved the use of the Microsoft Teams cloud-based phone system. This scenario typically involved convincing a hapless employee to install a remote access tool or other malware, which would then be used to further an attack. The actor **tinker** drafted the phishing scenario in just an hour.

Another **Black Basta** threat actor, **lapa**, was also charged with phishing-related operations. We discovered the gang possibly contracted several phishing-as-a-service (PhaaS) operators including the Ninja Admin phishing kit, a PhaaS program run by the persona **kalashnikov** aka **expert_kalash** and QuantumBuilder, which is a tool used to develop malicious .LNK files, also known as Windows shortcut files.

— Conducting malicious advertising (malvertising) campaigns via the Facebook and Google Ads services. The groupmember **lapa** was tasked with such operations in 2023. Malvertising is the practice of purchasing web advertisements intended to trick people into visiting malicious sites or links or downloading applications. The groupappeared to acquire Google Ads accounts from another cybercriminal actor.

Malware, tools used

The group commonly used third-party products as well as internally developed malware strains. Our research revealed the gang used the Anubis aka Bokbot, IcedID; Pikabot aka iPika; and Qakbot aka Qbot backdoors and malware loaders, which were not advertised on hacker forums.

Pikabot's development is proof of the proverb that necessity is the mother of invention. The group'sleader, **tramp**, was involved in administering and using the Qakbot loader malware during the actor's time with the **Conti** ransomware group, another one of the most destructive and profitable ransomware groups of all time. Qakbot was initial access malware that was used to load other malware onto a machine such as ransomware including Conti, ProLock, Egregor, REvil and MegaCortex. Qakbot spread in malicious spam or "malspam"

campaigns masquerading as invoices or interesting Excel files in hopes that victims would click through and launch a chain of events that would eventually surreptitiously install the malware. In 2022, Qakbot was absolutely prolific, posing daily challenges for large organizations that would receive floods of malspam.

Qakbot continued to be used by **Black Basta.** But Qakbot hit a roadblock in August 2023 when it was severely disrupted in an international law enforcement action. By that time, Pikabot had already been in development for about a year. The actor **tramp** had been collaborating with an associate, the actor **usernamew** aka **w**, to develop the Pikabot malware for **Black Basta's** exclusive use. The malware originally was codenamed iPika and frequently was referenced in the leaked conversations as "пика," which means "pike" or "knife" and is colloquial slang for the playing card suit of spades in the Russian language.

Despite a steady stream of improvements by **usernamew**, Pikabot never came close to the distribution scale of Qakbot. In February 2024, **usernamew** — who changed handles to **n3auxaxl** — expressed frustration that researchers reverse-engineered the malware quickly and referenced a report from cybersecurity vendor Zscaler on the new Pikabot version. The actor allegedly intended to implement additional obfuscation to hinder analysis. By May 2024, **n3auxaxl** planned to rewrite the source code and significantly upgrade the malware with a new name.

The group actively sought and tested other types of loader malware offered on underground forums. Two **Black Basta** members claimed to use AtomLoader. The group also used the Amadey malware loader, which the actor **InCrease** has promoted on the Exploit cybercrime forum since October 2018. The group'sarsenal also appears to have included private loader malware developed by the actor **lo0o0o0ong** and a private JavaScript loader from the actor **Baragozer**. The actor **tramp** also appears to have purchased the X.loader malware loader from the actor **Ghost_Pulse**; the EugenLoader aka FakeBat, PaykLoader, X.Loader loader from the actor **Payk_34** aka **eugenfest**; and the Matanbuchus loader from the actor **BelialDemon**.

Additionally, **Black Basta** member **usernameugway** claimed to purchase private loader malware from the actor **Bordislav**, who advertised the DarkGate malware loader in February 2024 and possibly was the actor **RastaFarEye's** alternative online persona or partner. The leaked chat logs confirm the **Black Basta** group also cooperated with **RastaFarEye** and purchased various malicious products from the actor.

Group members purchased antivirus (AV) software licenses to test malicious setups. They also purchased CrowdStrike, Sentinel and Sophos software to store on local servers to simulate real attacks.

Data exfiltration tactics

The group revealed numerous data exfiltration tactics used in 2023 and 2024, which varied depending on the available resources, targeted entities, amount of data and numerous other factors. The group allegedly used the Rclone and WinSCP services to set up file transfer protocol (FTP) servers and transferred data via the FileZilla service and the cURL command-line tool.

Another identified tactic was mapped drive exfiltration using RDP drive redirection or shadowing. The group configured local drives on its system to be accessible from a remote machine via RDP settings. This allows directly dragging and dropping files from the compromised machine to the attacker's local disk. The group members **adm** and **usernamegg** also used the pCloud secure file storage for stolen data.

Conclusion

The sheer diversity of tooling and techniques **Black Basta** usedmakes it a formidable adversary. It's impossible to have perfect defenses in place to block all of the attack vectors the gang used, whether it be malware, social-engineering attempts, malspam, compromised credentials or vulnerability exploitation. The group's leveraging of other offerings in underground cybercriminal forums and marketplaces proved to be a force multiplier, allowing it to use other capable tools to continue compromising victims.

Threat intelligence can help organizations stay ahead of attackers such as **Black Basta**. Understanding the latest malware, how it is distributed and how it functions can ensure better detection. Monitoring underground markets for offerings of compromised credentials can allow administrators to reset them before adversaries use them. Understanding which vulnerabilities may be of high interest to ransomware actors can ensure those flaws are either mitigated or patched properly.

Threat hunting — the practice of looking through logging systems for clues of a compromise — can potentially stop an attack from proceeding further. Intel 471's HUNTER platform contains pre-written queries that can be used to hunt for threats in endpoint detection and response (EDR), security incident and event management (SIEM) and logging systems. HUNTER contains a collection of hunt packages based on Black Basta TTPs. Register for a HUNTER Community Account, which contains sample free hunt packages and insight into HUNTER's comprehensive library of advanced threat hunting packages, detailed analyst notes and proactive recommendations. These resources are designed to strengthen your threat hunting capabilities and keep your organization secure.

For more information about how threat intelligence and threat hunting can thwart data breaches and ransomware attacks, please contact Intel 471.