From Royal to BlackSuit

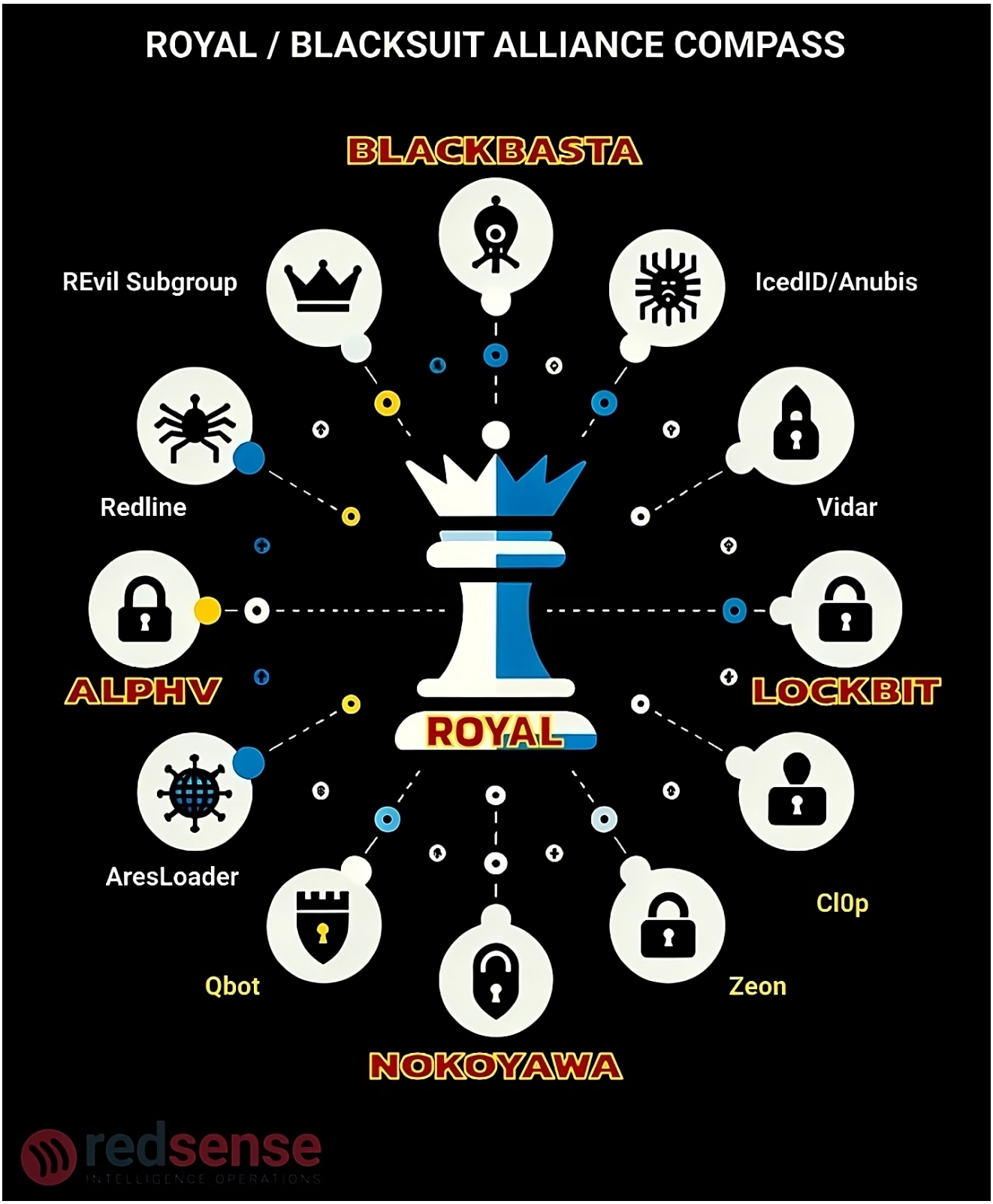
redsense.com/publications/royal-blacksuit-how-ransomware-rebrand-reshaped-them/

January 14, 2025

How a Ransomware Rebrand Reshaped Them

By Yelisey Bohuslavskiy, Marley Smith & Landon Rice

Introduction



BlackSuit has been one of the most advanced and prolific Russian-speaking ransomware groups for almost a decade (since the time they were named Team-2 within Ryuk ransomware). However, these days the groups are going through a painful transition marked by the internal struggle between the locker developer and the group's admin.

This struggle, which has already impacted companies with incidents such as their 2024 attacks against CDK Global, Kadokawa, and Niconico, originated during the complex process of the Royal-to-BlackSuit rebrand.

This journey could be characterized as a constant choice between encryption and exfiltration. In this research, RedSense relies on the adversarial perspective (i.e. the intelligence harvested from within adversarial infrastructure, both social and technical) to explain how the rebrand was shaped but also altered the larger Royal/BlackSuit history, and what critical characteristics of this group were revealed in this transition.

The first part of this research follows Royal's journey (October 2022 to October 2023), examining how this rebrand (October 2023 to October 2024) both follows and reinvents its operational legacy, shaping the trajectory of its future campaigns.

The second half follows the tools that characterized this rebrand: Over the past year, RedSense was able to recover samples of 10+ unique tools that are a mix of never-before-seen malware, off-the-shell "goodware" tools, commodity RATs, and an exclusive look at a new hand-built Command and Control (C2) framework that is in active use and development by the BlackSuit team to exploit and pivot in victim environments.

Royal's Journey

2022-2025

Formerly known as Conti-2 (as well as 'Quantum' for a short period following Conti's dissolution) BlackSuit has risen to become one of the largest and arguably most prolific active Russian-speaking ransomware groups. Known for major attacks on Costa Rica and the City of Dallas—and for triggering Conti's dissolution by openly siding with Russia—Royal built its reputation through a unique approach: centralized command with decentralized operations, adopting the best of Conti's structure.

Structurally, Royal built a "locker alliance," deploying a lineup of ransomware variants: BlackCat, LockBit, Quantum Locker (sourced from Mount Locker/Dagon), HIVE, Akira, and others. Their reach has since stretched beyond ransomware, as they monopolized Emotet and Anubis and established Royal's Malware Lab—a workspace for cross-group collective malware development.

By 2023, Royal's operations included a crew of 50 "pentesters" and a dedicated pre-attack team, harnessing call centers to reinforce BazarCall and constantly gathering intel through LinkedIn and insights into U.S. businesses for supply-chain infiltration. However, in October 2023, Royal executed a strategic rebrand, reemerging as BlackSuit—a shift that restructured their TTPs and arsenal (with a detailed analysis on this later in the report).

Prioritizing Exfiltration

October 2022 - March 2023

At the end of 2022, Royal had a firm reliance on botnets and legacy malware, essentially monopolizing **Emotet** by allegedly purchasing exclusive use of its source code and by deploying **Anubis** malware for its payload delivery.

Developing custom stealer tools—a theme that would continue to persist for the group—Royal partnered with elite **Initial Access Brokers (IABs)** in order to gain Citrix credential accesses and began to create an automated pipeline to streamline case handling. As the primary group exploiting critical vulnerabilities for **Apache Log4j**, Royal continued its CVE research, deploying novel **ProxyNotShell** and **MOVEit** zero-day vulnerabilities (which were also highly associated with **Cl0p**) to establish high-impact access points in corporate systems.

While encryption remained essential, Royal prioritized exfiltration. The group employed various families like **BlackCat, LockBit**, and **HIVE** as its associates to maximize damage to its victims' public image by posting on these groups' blogs. LockBit in particular amplified victim damages through public exposure tactics, with Royal posting massive blog posts for them and LockBit utilizing constant social media exposure and communication with journalists and security researchers to intensify the impact against victims.

Even their in-house locker tools, such as the Royal locker (based on the original Conti locker) and allies' malware like **Quantum** and **Dagon** (**MountLocker** line) served primarily as damage enhancers rather than primary components. Exfiltration, bolstered by targeted social engineering, was the real core of their strategy.

For this top priority, social engineering was integral to Royal's operations, and the group would leverage publicly available **LinkedIn** data to pinpoint high-value targets and craft personalized schemes to target victims' security and IT personnel. Their expansive call center and spam networks enabled the group to execute large-scale callback phishing attacks (aka **BazaarCall**), which involved Royal operators posing as legitimate services to trick victims into downloading malware. This blend of ransomware, botnets, and social engineering created a highly coordinated attack approach that defined Royal's activities from late 2022 to early 2023.

Keeping a "Social" Focus

January-March 2023

In early 2023, Royal ransomware executed three impactful social engineering campaigns which targeted a number of valuable sectors.

In February 2023, they used **black SEO** tactics to manipulate search engine results aimed at redirecting users searching for tech companies to a set of **fake websites**. This site prompted its visitors to download malware with the aid of a sophisticated chatbot, while Royal's partnership with a black SEO team bolstered their spam campaigns with extensive third-party data.

A similar campaign was political and impersonated a fictitious political group supporting a well-known candidate.

In March 2023, Royal intensified its phishing efforts by impersonating a fictional threat group ("**Midnight"**) to exploit high-profile U.S. companies. Victims were baited with a fake breach notice urging them to download a secretly malicious file ("*listing[.]rar*") which allegedly contained a listing of files taken from their system. Through a 500,000 email database, Royal's centralized server managed responses to these emails to use for future operations in order to maintain attack continuity. This campaign also introduced Royal's "**TrickBot-2**" loader, a Qbot alternative designed with advanced AV evasion, stealth, and Cobalt Strike integration for streamlined malware deployment.

May 2023: From New Loader to New Locker

On May 1, 2023, RedSense identified a new locker associated with the Royal's backend called **Blacksuit.** This locker was developed by the original creators of the Royal locker (from the *Ryuk-Conti-Royal* lineage, not the *AstraLocker-MountLocker-Quantum-Dagon* line). This locker was first tested in a small-scale attack on a New Jersey municipality.

A group internal update introduced the Blacksuit locker on May 1, followed by the the introduction of the **Gazavat stealer/CMD botnet** on May 2. A new malware loader, replacing .dll formats with .pdf and .doc files for more authentic phishing campaigns, was also tested during this period.

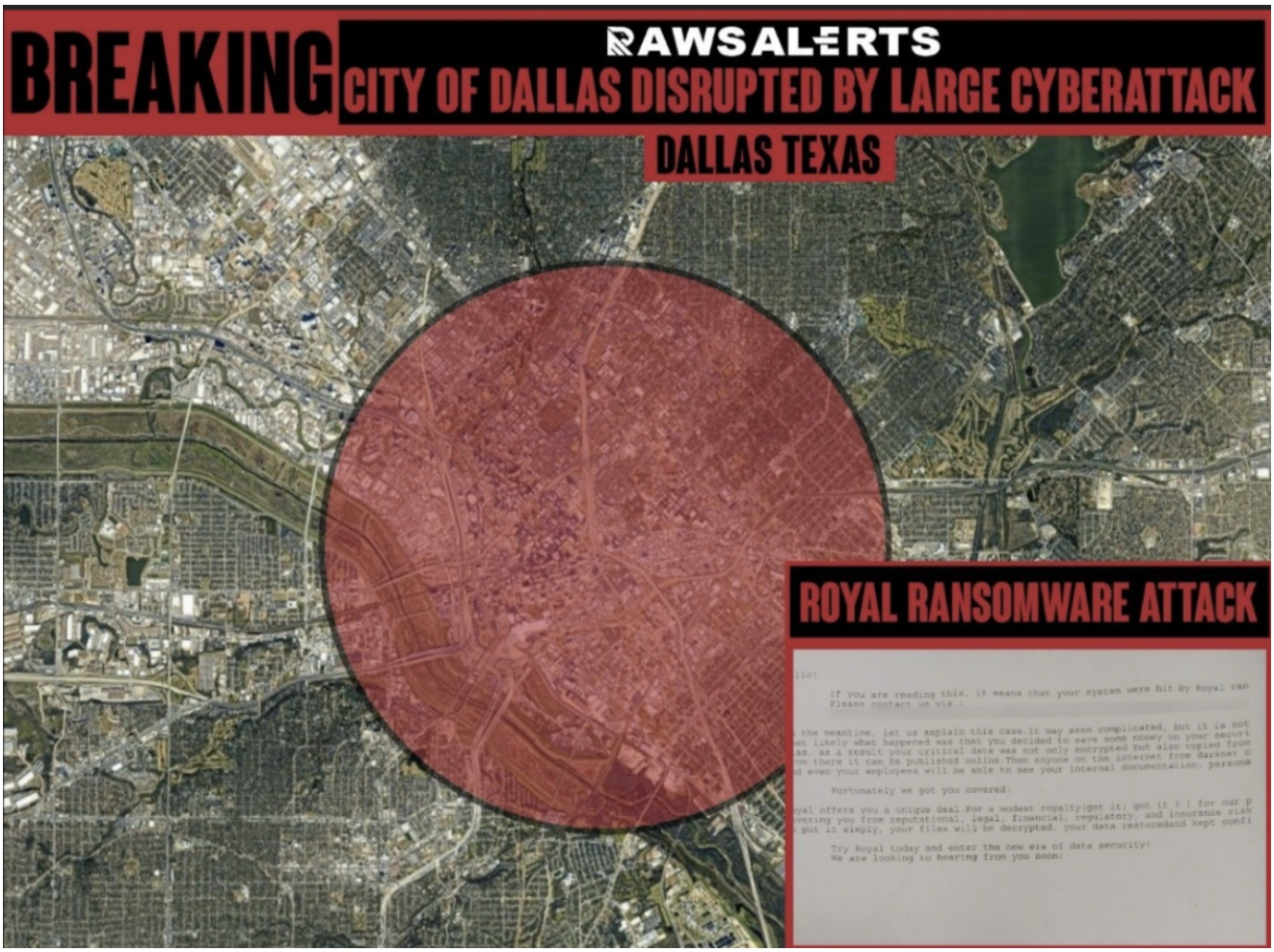


Image highlighting the affected radius for the city of Dallas, as well as featuring a copy of Royal's ransom note for the attack, via the media outlet. [Raw Alerts]

It is highly likely that Royal's leadership decided to rebrand as BlackSuit on May 1 intentionally, aiming to make their attack on Dallas as attention-grabbing as Conti-2's attack on Costa Rica in June 2022 (This earlier attack, led by the same Team 2 actors, served as a "finale" for Conti before its dissolution). At the same time, HUMINT suggests it was designed to assist the transition of Conti-2 into Quantum—Royal's predecessor.

The unusual tactics associated with this attack combined with Royal's timely structural updates led RedSense to assess with *moderate-to-high confidence* that the Dallas attack was a deliberate "stunt" designed to boost media visibility and introduce their new TTPs ahead of the group's rebrand into BlackSuit.

ROYAL TO BLACKSUIT

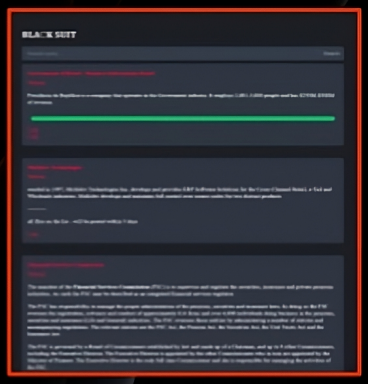
redsense
ACTIONABLE INTELLIGENCE REIMAGINED

PART-1

RYUK (2019) → CONTI-2 → QUANTUM → ROYAL → BLACKSUIT

2019 2022 2022 2023

ROYAL



BLACKSUIT

CHANGES & UPGRADES

Traditional Conti-centric payload — a shift from previous Quantum (a non-Conti MountLocker line) load

PAYLOAD

Also Conti-based, but with strong focus on ESXI exploitation

Was developed by March 2023, but took some time to be implemented properly

ROYAL

AKIRA | HIVE

ALPHV | EX-REVIL

LOCKBIT | EX-DARKSIDE

CENTRALISED IN OPERATIONS
DE-CENTRALISED IN COMMAND
BEST OF CONTI MODEL

-50+ Pentesters
-Utilizes others' lockers
-Consists of operators from many groups

ORGANISATION

BLACKSUIT

DEVELOPER | ADMIN

PENTERSTERS | ANALYSTS

SPAMMERS | CALLERS

-Very well-organized & hierarchical
-All members report to their "branch officer"
-Only deploy one locker

ROYAL TO BLACKSUIT

PART-2

RYUK (2019) → CONTI-2 → QUANTUM → ROYAL → BLACKSUIT

2019 2022 2022 2023

ROYAL

BLACKSUIT

CHANGES & UPGRADES

Diverse target profile

Publicly promised not to target education

Refrained from targeting medical facilities

VICTIMOLOGY

- UNPRECEDENTED NUMBER OF GOVERNMENT ENTITIES
- TARGETS MUNICIPALITIES SINCE MARCH 2023 INCEPTION
- MAY BE DIRECTLY RESPONSIBLE FOR DALLAS ATTACK
- DISPROPORTIONATE TARGETING OF EMERGENCY SERVICES AND EDUCATION

ROYAL PRECURSORS

- EMOTET
- ICEDID
- DARKGATE
- ARESLOADER
- GAZAVAT
- TRICKBOT-2
- PROXYNOTSHELL CVE
- RE-WEAPONIZED REDLINE & VIDAR
- ALPHV-STYLE LINKEDIN PARSING

KILLCHAIN

- PRIMARILY RELIES ON INITIAL ACCESS BROKERS
- NO MASS PHISHING CAMPAIGNS
- RELIES HEAVILY ON CALL CENTERS
- PRIORITIZES POST-BREACH OPERATIONS
- CITRIX BLEED CVE

Refocusing on Encryption

June 2023-October 2023

The transition to BlackSuit (still unofficial at the time) marked a significant shift in Royal's tactics, moving toward a more traditional encryption-oriented approach. This was a departure from their focus earlier in 2023, where Royal still prioritized exfiltration.

Royal's shifts between the encryption and exfiltration focus are closely tied to its origins in the Conti syndicate. Conti as a group began by adding a public shame blog to Ryuk. This was a controversial decision at the time, as early Ryuk operatives (who later formed groups like **Zeon, Akira**, and **Play**) preferred sticking to encryption-only attacks. However, the group admin (who would later lead Conti2/Royal) advocated for a novel, more exfiltration-centric approach with the introduction of Conti's leak blog, which became highly successful.

This same admin, however, later used the blog to promote political agendas supporting Russia, which was a significant factor leading to Conti's dissolution. The fallout left many ex-Conti operatives skeptical of the blog-centric model, favoring encryption as their primary tactic.

While Royal leaned on exfiltration and maintained a blog, other Conti offshoots, like Conti-4 and Conti-5, focused on the Asian and LATAM (Latin American) darkweb markets, while groups like Zeon and Silent Ransom prioritized encryption. Royal's competitor, BlackBasta (Conti-3), struck a balance by maintaining a prolific active blog while still heavily focusing on encryption and operating a separate exfiltration-only arm, **Karakurt**. By Spring 2023, Royal began navigating the ongoing shifts in the locker ecosystem, refocusing from exfiltration and social engineering toward a more balanced strategy.

The development of BlackSuit reflected this shift.

By mid-2023, Royal initiated a bid for a new locker in the form of a competition, with contributions from Akira as well as former Ryuk developers. While the precise origin of BlackSuit remains unclear, it was selected after testing and became central to Royal's strategy. Alongside BlackSuit's introduction, Royal recruited an elite group of former **REvil** pentesters who were known for their high-profile breaches to enhance their encryption capabilities. This internal pivot signaled a return to encryption as a core tactic while maintaining exfiltration as a supplementary pressure strategy.

Simultaneously, Royal began working on new delivery tools for the new locker. On July 19, 2023, RedSense confirmed that Royal had armed its loader for the next phase of testing. This update involved the distribution of 300,000 spam emails containing the active **Cobalt Strike DLL** payload.

By August, Royal had advanced and updated its malware loader, now called **Trick3**, specifically for this campaign. Trick3 leveraged the use of ActiveX objects, which were hidden as an Adobe Acrobat update prompt on a PDF invoice which was sent to victims. Clicking these ActiveX objects would execute the loader to deliver Royal's malware payloads. Finally, by October 2023, Royal finally completed its rebrand and became BlackSuit.

As seen above, this transition was not just a simple rebrand, but a long-calculated strategic move. The most important thing, however, was that the group began prioritizing encryption over exfiltration again, and this resulted in more power held by the locker developer. This itself lead to the crisis of command between BlackSuit's admin and the locker developer which is incremental to the current group's tactics.

BlackSuit's Toolkit: Tools that Enabled the Group's Rebrand

By Landon Rice with contributions from Marley Smith

TOOL #1- ARESLOADER

- **NAME:** icsnd1.exe
- **TYPE:** PROPRIETARY MALWARE
- **DEFENDER DETECTED:** YES
- **VT DETECTED:** YES
- **SUMMARY:** A malicious loader which has been extensively advertised on the darkweb, namely RAMP and XSS forums, by the threat actor "DarkBLUP".

Tool Analysis & Notes

As of 2024 BlackSuit was aiming to recreate the Emotet-TrickBot-Ryuk killchain by implementing a combination of AresLoader-Lumma-BlackSuit.

BlackSuit and Royal leadership saw AresLoader as an alternative to Emotet. This is a relatively simplistic loader which has been in use since early 2022, and originally sold licenses to threat actors using a monthly subscription model for 300 USD per month.

NOTE: The loaders should not be confused with the open-source loader "**Project Ares**", which written by redteamer *"cerbersec"* as a **PoC (Proof-of-Concept) which implemented the Transacted Hollowing Injection technique.**

Ares Loader's sole functionality is calling down a file from the internet and running it while attempting to masquerade as a legitimate binary. Loaders like these are very common on the darkweb, giving cybercriminals an easy way to prevent detection of their commodity and often open-source malware/stealers. The loader implements some basic anti-analysis techniques, but ultimately does not stand out within BlackSuit's extensive toolkit.

TOOL #2- LUMMAC2 STEALER

- **NAME:** MED.exe
- **TYPE:** ILLICIT COMMERCIAL STEALER
- **DEFENDER DETECTED:** NO
- **VT DETECTED:** YES
- **SUMMARY:** Lumma Stealer (aka LummaC2 Stealer) is an infostealer written in C that has been available through a Malware-as-a-Service model via Russian-speaking forums since around August 2022.

Tool Analysis & Notes

As of 2024 BlackSuit was aiming to recreate the Emotet-TrickBot-Ryuk killchain by implementing a combination of AresLoader-Lumma-BlackSuit.

RedSense analysts discovered a LummaC2 payload among BlackSuit's original arsenal introduced on their internal assets in May 2023. This is a highly advanced infostealer that is in active development today, and is a favorite tool of many cybercriminals. This stealer has an incredibly active Telegram and darknet presence, and is run by the threat actor *"Shamel"* under the alias *"Lumma"*, which the product is named after.

The stealer has a strong emphasis on stealing **two-factor authentication codes** and **cryptocurrency wallets** from a wide range of extensions across a wide range of browsers. Once it gathers all of the data off the victim machine, it POSTs the data (over raw HTTP) to its C2 server with the *"TeslaBrowser/5.5"* user agent.

RedSense has seen a wide range of stealers in use across a wide range of ransomware gangs, but this specific combination of BlackSuit and Lumma has not been publicly disclosed or widely analyzed.

This subscription-based infostealer implements a wide range of available payloads, including EXEs, DLLs, PowerShell Scripts, and is often deployed via a loader, either provided by the Lumma developer(s), or custom written. The heart of the stealer is quite evasive, and is some of the highest-tier malware that is publicly available.

The tool implements its own form of API Hashing , and uses Anti-Sandboxing/Anti-Debug checks , Control Flow Obfuscation , Heaven's Gate Technique , (In)direct syscalls , and a long list of other evasion techniques that are consistently updated and changed based on detections. The malware author(s) verify and check each release against Windows Defender, and ensure it is not detected at the time of release. Even with all of these techniques, Lumma highly recommends using a crypter/loader upon execution, to minimize the chances of detection, and getting leaked.

NOTE: After RedLine takedown, Lumma is considered the number one priority stealer among the Russian-speaking ransomware leadership.

TOOL #3- CUSTOM C2

- **NAME:** fuckallav.ru
- **TYPE:** PROPRIETARY MALWARE
- **DEFENDER DETECTED:** NO
- **VT DETECTED:** NO
- **SUMMARY:** A developmental C2 by BlackSuit's team, allowing for SOCKS, keylogging, screen recording, command execution, and custom sleep time.

Tool Analysis & Notes

During analysis, RedSense analysts discovered evidence of a custom Command and Control framework that was in a developmental stage by BlackSuit's Malware Development team. Very few Threat Actors put in the time and energy to develop their own custom C2 framework, and this speaks to BlackSuit's sophistication and investment in their craft.

The C2 panel contains the following functionality:

- **Bots-** The home page of the C2, showcasing all of the victims, along with their unique bot ID, IP address, and comments.
- **Files-** Allows the operator to view saved/exfiltrated files from the victim's machine.
- **Send Commands-** Contains a list of active victims and a text input box to run custom commands on selected victims.
- **Send Comment-** Not shown, but we can assume it allows operators to add custom "notes" or tags to a victim.
- **Keylogs-** Not shown, but we can assume it allows the operator to view exfiltrated keystrokes for each victim.

- **Admins-** Not shown. Likely supports multi-user capabilities for the panel.
- **Switch the language to ru-** Self explanatory. Hints that the original developer may be of Russian origin.
- **Mail spam-** Mail spamming feature, allowing operators to send emails/phishes from the panel.
- **Exit-** Closes the tab for the C2.

For the malware itself, RedSense discovered the following commands/capabilities:

1. *!On/Off- Activation/deactivation of the malware*
2. *!CMD - execution of the command in Windows CMD*
3. *!Time - Changing the sleep time of the bot*
4. *!Getdir - Get directory listing of the system*
5. *!SCR - turning on the mode of sending the screen broadcast using periodic screenshots*
6. *!SOCKS - Configuring/installing SOCKS proxies*
7. *!@Url - Downloading, and unpacking the file if it's a .zip. Then proceeds with execution, if it is an executable file, or registration in the system, if it is a DLL.*
8. *!KLG - Activation or deactivation of the keylogging function.*

TOOL #4- ZENPAK MALWARE

- **NAME:** Alinstaller.exe
- **TYPE:** UNATTRIBUTED BACKDOOR
- **DEFENDER DETECTED:** NO
- **VT DETECTED:** YES
- **SUMMARY:** This piece of malware does not match any signatures of known malicious software.

Tool Analysis & Notes

Alinstaller.exe (identified within the adversarial infra) does not match any 1:1 signatures for known viruses, though it does have multiple malicious functionalities which were discovered by RedSense. VirusTotal, among other engines, give it conflicting attribution names,

including **TrickBot, Sefnit, Artemis**, and **Waledac**, although the most common attribution for this file is "**Zenpak**". "Zenpak"'s functionality includes:

Alinstaller.exe

- Contains self-spreading and self-replication capabilities.
- Contacts domain "ip-api[.]com" to grab victim's IP address.
- Accesses and manipulates PEB_LDR_DATA data structure for evasion.
- Implements multiple forms of anti-sandbox and anti-debug technology.
- Encodes and Decodes data with XOR.
- Logs keystrokes via application hooks and polling.
- Manipulates Powershell-related registry keys.

TOOL #5- COBALT STRIKE (LICENSED COPY)

- **NAME:** Cobalt Strike v.4.6
- **TYPE:** COMMERCIAL PENTEST TOOLING
- **DEFENDER DETECTED:** YES
- **VT DETECTED:** YES
- **SUMMARY:** Cobalt Strike is a powerful, extensible penetration testing platform that provides security analysts with an interactive analysis workspace and a variety of tools for attack simulation, exploitation, post-exploitation, and report generation.

Tool Analysis & Notes

RedSense's analysts discovered multiple compiled Cobalt Strike beacons alongside the original BlackSuit infrastructure (introduced in May 2023). It contained a *legitimate, licensed* copy of the Cobalt Strike framework. (**NOTE:** *While seeing threat actors using Cobalt Strike is common, it is very rare to stumble across a group utilizing a genuine copy of the software. The majority of lower-tier actors share leaked and/or cracked copies.)*

This speaks to BlackSuit's high level of sophistication in their ability to gain access to an up-to-date and recent version of the software, as opposed to older (and backdoored) copies that are generally shared around the darkweb. This copy was seen to be using the following **arsenal kits:**

Applet Kit: Allows operators to modify Cobalt Strike's built-in Java Applet payloads. This kit was the first to be added to Arsenal and is no longer widely used.

Artifact Kit: Allows operators to modify the templates for all Cobalt Strike executables, DLLs, and shellcode.

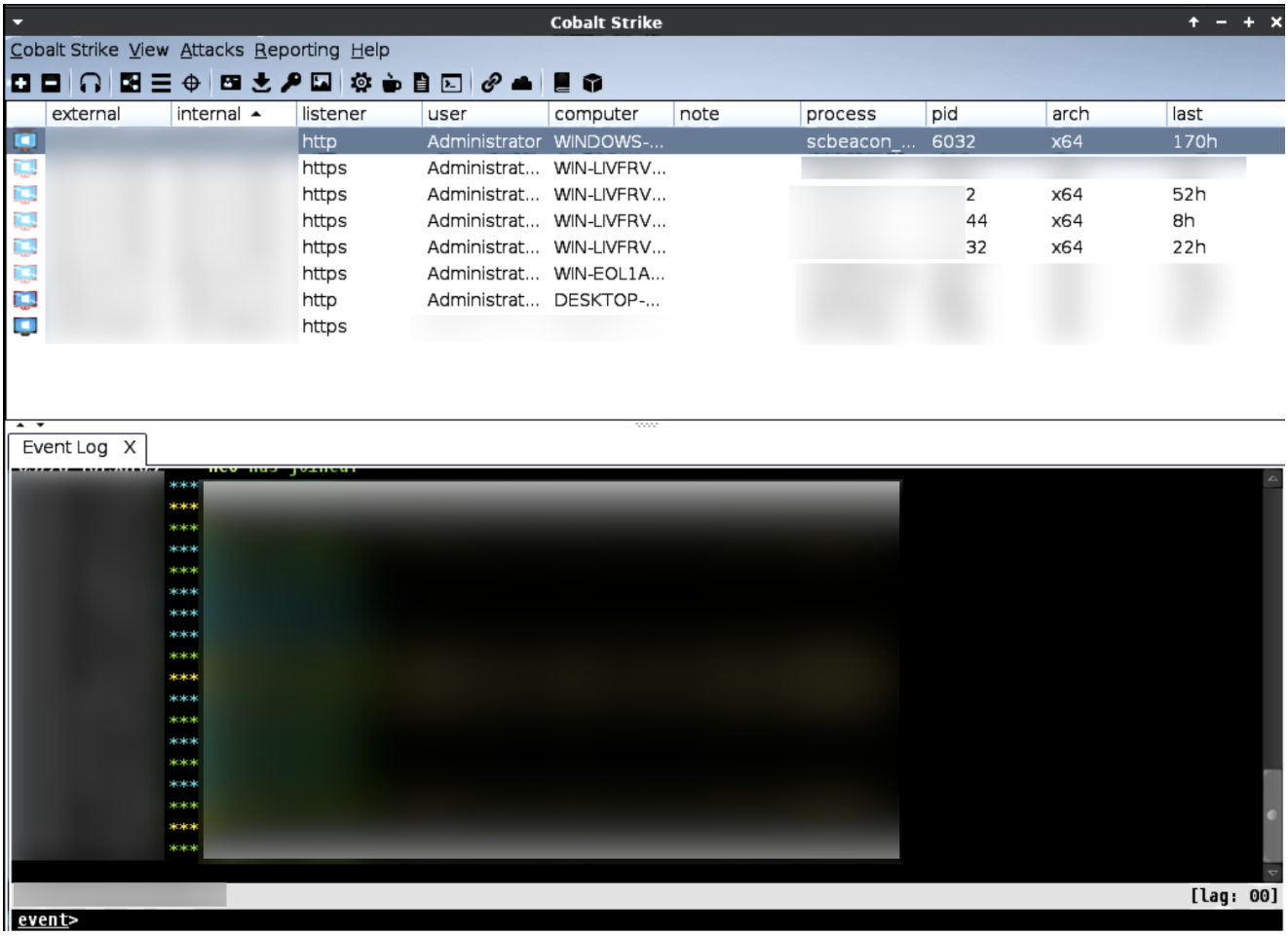
Mimikatz Kit: Allows operators to update their version of Mimikatz without waiting for a Cobalt Strike software update. Mimikatz is a very popular tool used to dump credentials on Windows machines.

Power Applet Kit: This is an alternate implementation of Cobalt Strike's Java Applet attack that uses PowerShell to get a payload into memory.

Resource Kit: The Resource Kit is Cobalt Strike's means to change the HTA, PowerShell, Python, VBA, and VBS script templates Cobalt Strike uses in its workflows.

Sleep Mask Kit: The Sleep Mask Kit contains options for the sleep mask function that is executed to obfuscate Beacon in memory, prior to sleeping.

Reflective Loader Kit: This allows operators to customize the reflective loader functionality used by the core beacon, allowing for operators to implement new evasion techniques.



Redacted screenshot of BlackSuit's Cobalt Strike control panel [source: RedSense]

TOOL #6- PROXIFIER

- **NAME:** proxifier.lnk
- **TYPE:** GOODWARE
- **DEFENDER DETECTED:** NO
- **VT DETECTED:** NO
- **SUMMARY:** Proxifier is a program that allows network applications that do not support proxy servers to operate through a SOCKS/HTTPS proxy or a chain of proxy servers.

Tool Analysis & Notes

Proxifier is a tool that can be used to tunnel all network connections through a proxy, making it an attractive option for threat actors looking to pivot deeper into an environment. By turning a victim machine into a proxy and routing all of their traffic through it, actors can access deeper and segmented parts of a network to continue their attack. This can make it very difficult to identify and stop cybercriminals before they cause significant harm. Proxifier allows threat actor to:

- Run any network applications through a proxy server (No special configuration is required for the software).
- Access the Internet from a restricted network through a proxy server gateway.
- Bypass firewall restrictions.
- “Tunnel” the entire system (force all network connections including system connections to work through a proxy server).
- Resolve DNS names through a proxy server.
- View information on current network activities (connections, hosts, times, bandwidth usage, etc.) in real-time.
- Maintain log files and traffic dumps.
- Get detailed reports on network errors.

TOOL #7- SOFTPERFECT NETWORK SCANNER

- **NAME:** netscanold.exe
- **TYPE:** GOODWARE
- **DEFENDER DETECTED:** NO
- **VT DETECTED:** NO
- **SUMMARY:** Powerful multipurpose network administration tool, with the ability to scan both the IPv4 and IPv6 network space.

Tool Analysis & Notes

The SoftPerfect Network Scanner is a closed source network scanning tool. SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders and retrieve information about network devices via WMI, SNMP, HTTP, and SSH. It also scans for remote services, registry, files and performance counters, and offers flexible filtering and display options with the capability to export NetScan results to a variety of formats from XML to JSON.

This sample was configured with the *following data:*

Scan of TCP Ports: 445, 1433, 2179, 3389, 6160, 5000, 5001, 6101, 9392, 9393, 9443, and 9401

Get Banners from Ports: 21, 80, 443, 3128, 8080, and 16992

Scans of the following IP ranges:

- *10.10.0.0/16*
- *10.20.0.0/16*
- *10.30.0.0/16*
- *10.40.0.0/16*
- *10.50.0.0/16*
- *10.211.0.0/16*

TOOL #8- PCHUNTER

- **NAME:** PCHunter64.exe
- **TYPE:** GREYWARE
- **DEFENDER DETECTED:** NO
- **VT DETECTED:** YES
- **SUMMARY:** Toolkit with access to hundreds of settings including kernels and kernel modules, processes, network, startup and more.

Tool Analysis & Notes

PCHunter is a powerful tool designed to give users broad access and control over Windows operating systems. Hackers can use PCHunter to control critical system components. With the ability to manipulate kernel structures and interfere with system processes, malicious actors can use PCHunter to abuse the lowest level of access to deal damage to a victim PC. Some of the tool's capabilities include:

Process Viewer: Can be used to view sensitive information such as passwords, credentials or personal data stored in memory and steal it.

Kernel Module Viewer: Can be used to load and unload kernel modules, as well as view their memory.

Hook Detector: Can be used to hook view hooked system calls, allowing an attacker to detect anti-virus software.

System Callback Viewer: Can be used to view kernel callbacks, shutdown events or file system notifications.

Network Viewer: Can be used to view sensitive network traffic or intercept data being transmitted over the network for malicious purposes such as stealing credentials or personal information.

Registry Viewer: Can be used to modify system settings, delete important registry keys or install persistence onto a victim host.

TOOL #9- RUBEUS

- **NAME:** rubeus.exe
- **TYPE:** OPEN-SOURCE PENTEST TOOL
- **DEFENDER DETECTED:** YES
- **VT DETECTED:** YES
- **SUMMARY:** Rubeus is a C# toolset for raw Kerberos interaction and abuses.

Tool Analysis & Notes

Rubeus is a C# executable and library built to interact with the Windows AD Kerberos protocol. This software, built by security researcher Will Schroeder , is a common method for threat actors to use and abuse Kerberos across Windows environments.

Similar to mimikatz , Rubeus includes a long list of commands to interact with **Kerberos tickets.** This includes creating, forging, bypassing, requesting, retrieving, managing, harvesting, roasting, extracting, and otherwise manipulating them. It is not uncommon for threat actors to use Rubeus to leverage these capabilities, as it is a useful tool for **exploiting Active Directory environments.**

TOOL #10- DOMINO (MINODO)

- **NAME:** x64.exe
- **TYPE:** PROPRIETARY MALWARE
- **DEFENDER DETECTED:** YES
- **VT DETECTED:** YES
- **SUMMARY:** Domino, also referred to as Minodo, is a custom backdoor developed by Fin7 and Ex-Conti actors.

Tool Analysis & Notes

This strain of malware, Domino, has been extensively analyzed by **IBM's X-FORCE** team. This backdoor registers itself with a Command and Control server, encrypts communications with AES, and allows operators to load additional tools, namely the Nemesis Infostealer and Cobalt Strike.

Domino/Minodo first discovered in early 2023, and has been seen multiple times since, often being deployed by Royal, BlackBasta, and other ex-Conti ransomware groups. This hints at the fact that one/many of the core developers may be working with BlackSuit.

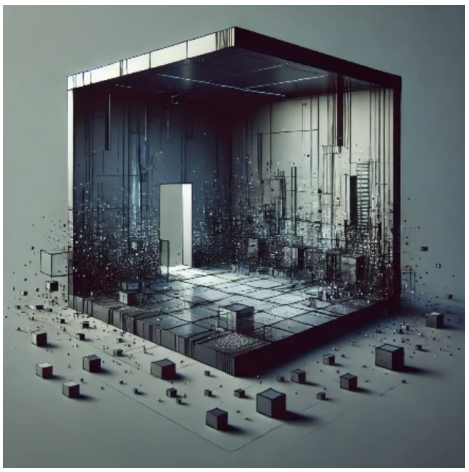
MISCELLANEOUS TOOLS

- **TITLE:** WINSCP
- **NAME:**
  winscp.lnk

- **TYPE:** GOODWARE
- **DEFENDER DETECTED:** NO
- **VT DETECTED:** NO
- **SUMMARY:** Free and Open-Source file transfer tool that can communicate over (S)FTP, FTPS, SCP, WebDAV or S3 file transfer protocols. Often used by Threat Actors for data exfiltration.

- **TITLE:** GMER ROOTKIT DETECTOR
- **NAME:**
  gmer.exe

- **TYPE:** GREYWARE
- **DEFENDER DETECTED:** YES
- **VT DETECTED:** YES
- **SUMMARY:** Application that detects and removes rootkits. Can find hidden processes, threads, modules, services, files, disk sectors, data streams, registry keys.



- **TITLE:** VIRTUALBOX
- **NAME:**
  Oracle_VM_VirtualBox_Extension_Pack-6.1.16.vbox-extpack

- **TYPE:** GOODWARE
- **DEFENDER DETECTED:** NO
- **VT DETECTED:** NO
- **SUMMARY:** Expands the functionality of interaction between a guest virtual machine and a host machine after installation inside the guest machine.

- **TITLE:** PASSWORD TOOL
- **NAME:**
  Password Tool.exe

- **TYPE:** GOODWARE
- **DEFENDER DETECTED:** NO
- **VT DETECTED:** NO
- **SUMMARY:** Tool to quickly and easily change the password of the current user.

- **TITLE:** POWERTOOL
- **NAME:** PowerTool64.exe

- **TYPE:** GOODWARE
- **DEFENDER DETECTED:** NO
- **VT DETECTED:** YES
- **SUMMARY:** PowerTool is a free anti-virus & anti-rootkit utility. It offers you the ability to detect, analyze and fix various kernel structure modifications and gives you a wide scope of the kernel.

IOCs

All relevant IoCs are included in RedSense's IoC database for service subscribers.

Hashes	*8f9760226b17030371fad2539a98ce7a* *955ecf3cd5b8562dd610b2daac413e99* *bd61059259bf5208509d15726ce5dfab* *300bd29c8639ebe794d2dd449d49fdca* *3069012ec13cf5043829dfdcc52be0c2* *bf843074cb5e61ca955ba3c30019c24b* *82d0eddf99ab5f8dea209d756ba13c4a* *2cc79806701f1a6e877c29b93f06f1bb* *171d8bdb16f062f3a84310b37622a4d3* *1e819c99570a76695cdbd66b8e49d432* *75f3b2d0dac980275b94b1dbbf080d52* *be0e1b863340b5d3f980b614a7118b11* *f40646272ff1f8f5e8d7021276d78841* *5f8bea9e93432e5eaf7df2ccf7c7a7ac* *6798ff540f3d077c3cda2f5a4a8559f7* *b2fcaffce69d5a32de53db54ed5c3a7c*
IPs	• *79[.]132.129.137* • *88[.]119.175.124* • *79[.]141.162.131* • *85[.]239.54.214*

Emails/Personas	• *jekkymacros@xmpp[.]jp* • *shahaburin@yandex[.]ru* • *7555@yopmail[.]com* • *frencisbetorv@hotmail[.]com* • *germanbuss@proton[.]me* • spy