

Sophos 2023 Threat Report

# Maturing criminal marketplaces present new challenges to defenders

Sophos X-Ops

# Contents

<b>Letter from the CTO</b>	<b>2</b>
<b>Setting the tone: The war in Ukraine</b>	<b>4</b>
A regional conflict echoes worldwide	4
At the center of things	5
<b>Malware economics</b>	<b>6</b>
A naughty nine	6
Maturing from 133t to slick	11
Infostealers	13
<b>Ransomware evolution</b>	<b>17</b>
<b>Attack tooling</b>	<b>20</b>
<b>Turning offensive security tools to bad ends</b>	<b>21</b>
Other abused security tools	24
Dual-use RATs	24
LOLBins and legitimate executables	25
"Bring your own" vulnerabilities	26
Ransomware targeting endpoint-security upgrades	28
Miner malware	28
<b>Beyond Windows: Linux, Mac, and mobile threat landscapes</b>	<b>30</b>
Linux threats	30
Mobile threats	33
<b>Conclusion</b>	<b>34</b>

**Joe Levy**

Sophos CTO

## Letter from the CTO

The cybersecurity industry tends to look back at the end of the year, every year, and pronounce the past twelve months as among the most consequential time in the history of the industry. While 2022 hasn't had a branded event the likes of Aurora, Stuxnet, WannaCry, or the Colonial Pipeline cyberattack, it unfortunately earned its place in the annals of cyberhistory as a war erupted in Europe – the largest in a half century.

Why this matters to cybersecurity is that a country well known as one of the world's principal promoters and safe havens of cybercriminal activity, the primogenitor of ransomware as a de facto national industry, invaded its neighbor.

Once Russia invaded Ukraine, it was inevitable that the Russian government would, if not draft into service, strongly encourage its homegrown cybercriminal enterprise to spin global opinion in its own favor while attempting to sabotage the goodwill Ukraine's president may have built up around the world. Which is exactly what happened when ransomware, malware, and disinformation groups all spun up in support of Russian aggression.

That effort, so far, has been an utter failure. Global opinion of ransomware criminals was already at rock bottom when, throughout the pandemic, gangs targeted the most vulnerable parts of the business sectors most crucial for mounting a response, including the healthcare industry, medical research organizations, businesses critical for maintaining supply chains and food and energy operations, and even educational systems. They hadn't exactly built a wellspring of goodwill for themselves when ransomware gangs further angered the world by pronouncing their unwavering support of Russia's invasion and declaring as targets any country or organization that opposed them.

But other members of those same gangs, based in Ukraine, saw things a little differently. And a tit-for-tat war of leaks began, revealing some of the most sensitive information ever disclosed about how ransomware threat actor groups operate. The war seemingly severed the ties between Ukrainian threat actors and their Russian (and Belarussian) counterparts, possibly permanently.

At the same time, during this period in which Russia has been preoccupied promoting its war of aggression, China has been making dramatic cybercriminal moves, targeting not only its neighbors and the countries it considers crucial in its "belt and road" initiative, but the security industry itself. In an increasingly brazen set of attacks against the companies on the front lines of protecting information and networks, China-based (and likely sponsored) threat actor groups have been attacking the hardware security products made by nearly every company in the cybersecurity and infrastructure industries.

In a very real, and very personal sense, it feels like the gloves have come off in 2022, and the two largest nations that pose a cybersecurity threat to the rest of the world have decided to do away with the pretense of noninvolvement in large breaches, major attacks on infrastructure, or disruption to education, global commerce, or healthcare. They might as well be flaunting it in our faces, as if to demand what are you going to do about it?

What we have been doing about it, and what Sophos will continue to do about it, is to bolster our initiatives already underway to protect both our customers and ourselves. The company has been taking on a multi-year process of incrementally improving detection and automated intervention of ransomware behavior, becoming so successful at sabotaging attackers that those active adversaries now increasingly turn their efforts to evading us before they can make good on any threats.

At the same time, in light of attacks against security infrastructure by both China- and Russia-based threat groups, trust in our vendors matters more than ever before. We believe that vendors must transparently communicate their investments in security for that trust to be earned and maintained, particularly when the vendor is in the business of providing cybersecurity services and products. Sophos maintains a [Trust Center](#) for insights into the work we do around advisories and disclosures, our security testing and bug bounty program, and our incident analysis and response plans. We make continual investments in protecting our own infrastructure against targeted attacks by APTs, and hardening the hardware and software that runs in our customers' environments. Success in this regard will be incremental, as the adversaries have not stopped trying to discover and exploit vulnerabilities, and in fact seem to have stepped up efforts designed to subvert the security of every vendor's firewalls, switches, and network access points. We also continue to push secure-by-default configurations into our offerings, and introduce conveniences such as health checks and policy remediations into our products and services to improve operating postures and hygiene.

Threats will continue to evolve, and Sophos will relentlessly adapt to continue to deliver superior cybersecurity outcomes.

## Setting the tone: The war in Ukraine

If war is the continuation of politics by other means, and cyber-conflict is just another branch of warfighting, it makes sense that the Ukraine conflict looks similar online and off. At this writing, the threat landscape looks ugly within the borders of Ukraine, while causing less pervasive but still significant disruption in the rest of the Western world – and unease, as the potential for wider conflict, disinformation, and disruption remains high.

### A regional conflict echoes worldwide

As one would expect, the February 24 kinetic escalation of Russian attacks on Ukraine brought out the scammers looking to profit from global grief and concern.

In early March, we [tracked](#) an uptick in fake charity emails requesting international donations for Ukraine. In those first days of the war, Ukrainian officials made appeals to the world for donations to help with their defense efforts, and those appeals included requests to donate cryptocurrency to the country's treasury. Scam artists immediately latched on to the cryptocurrency angle and sent millions of spam email messages that echoed the request, but swapped out the cryptocurrency wallet addresses to include ones not associated with the government, or any other legitimate charity or nongovernmental relief agency. Over the weekend of March 5-6, the volume of spam soliciting donations to these bogus cryptocurrency wallets was so large it made up fully half of all spam we received in that time period – a shockingly large quantity. Fortunately, the campaign died down within a few days.

### Ukraine scams as a percentage of daily spam volume, March 2022

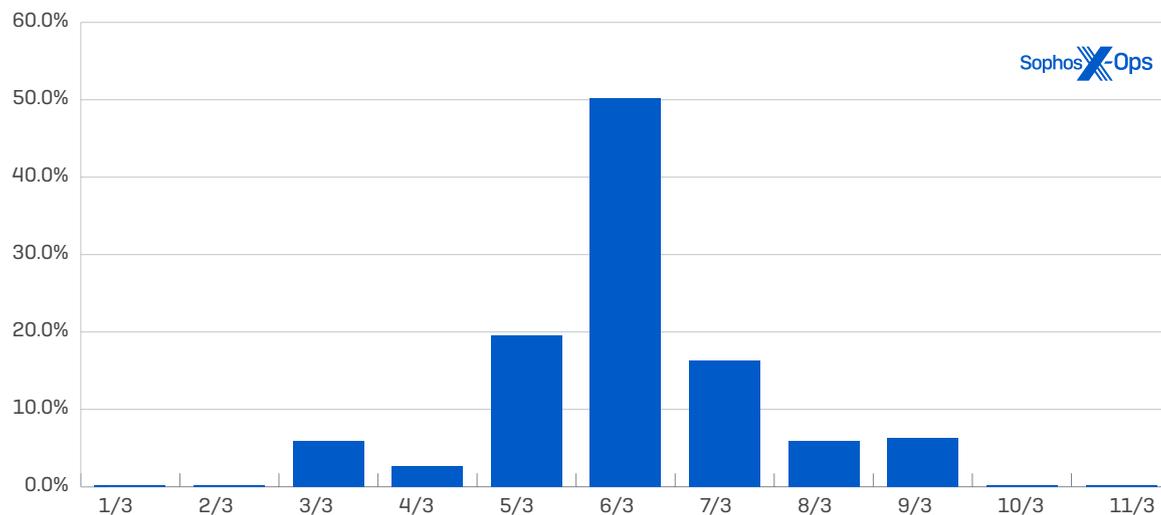


Fig.1. The volume of spam emails soliciting donations to bogus cryptocurrency addresses spiked sharply, though briefly.

By May there were also hundreds of fake sites requesting “donations,” but as with the initial spam, based on commonalities in financial information these were probably run by relatively few entities. The driving factor in these attacks was not great technical sophistication. Instead, attacks invoked the country's name or those of its leadership as part of social engineering lures, relying on relatively old vulnerabilities and exploits to follow through.

For example, in one [notable](#) spam campaign that month, the [Emotet](#) malware group distributed a collection of malicious Word documents with provocative titles that mimic Russian propaganda, such as “US and Allies provide chemical weapons to Ukraine's military.doc,” in an attempt to spread their malware. The malicious documents in that attack leveraged a [CVE-2021-40444](#) exploit to infect the computers of victims who opened the documents on machines that had not installed that Office patch, which had been released the previous fall.

Name	Date modified
 Chemical weapons use from Syrian war stokes Ukraine's fears.docx	5/10/2022 2:43 AM
 list of nato generals hiding in the basement of the Azovstal steel plant.docx	5/10/2022 2:46 AM
 Nato's generals who were hiding in the underground bunker of the Azovstal steel factory just surrendered.docx	5/10/2022 2:47 AM
 The US Violation of the Chemical Weapons Convention.docx	5/10/2022 2:44 AM
 Ukraine war Fact-checking Russia's biological weapons claims.docx	5/10/2022 2:43 AM
 US aircraft carrier approaches the black sea to support Ukraine.docx	5/10/2022 2:48 AM
 US and Allies provide chemical weapons to Ukraine's military.docx	5/10/2022 2:46 AM
 US 'deeply concerned' at report of Mariupol chemical attack.docx	5/10/2022 2:44 AM
 US, Allies Probe Claim of Chemical Agent in Ukraine.docx	5/10/2022 2:45 AM



Fig. 2. Document titles in malicious Ukraine-themed Emotet spam made false and frightening claims.

As for state-level cyberattacks outside Ukraine's borders, at this writing the attribution of one of the two highest-profile incidents is less than solid. The ViaSat attack, which affected satellite services for Ukrainians and also for customers elsewhere in Europe hours before the invasion began, is firmly [credited](#) by officials as Russia's work. But the October defacements of public-facing airport web sites in the West are harder to interpret: Were these nation-state efforts to intimidate Ukraine's allies, or were they freelance attacks?

It's sensible, in fact, to operate as if it is the latter. Low-tech defacements and DDoSing (including on airport sites, not to mention the attempt to disrupt Eurovision voting) were another feature of the early days of the war, but as the conflict drags toward another winter and global tensions are high, some non-technical observers found the site-bothering antics of Russia-affiliated KillNet— a reminder that nothing on that front is yet resolved.

## At the center of things

Inside Ukraine, the picture is darker and stranger. Several attacks targeting the Ukrainian government have followed patterns seen in criminal campaigns – the use of social engineering emails, commodity malware, and abused commercial offensive-security tools. In one case, a forged email contained a link to an “antivirus update” that instead dropped a beacon for Cobalt Strike. In another (which we'll look at later in this report), an information thief claimed to be selling large amounts of data on Ukrainian citizens and government organizations – no known ransom demand, just breaching to expose data.

Meanwhile, Ukraine and Russia, though they are separate countries, have citizens who have been longtime partners in (literal) crime, with multiple ransomware gangs using affiliates based in both nations. When war broke out, certain gangs apparently fell apart in bursts of nationalism.

Most spectacularly, divisions between Russian and Ukrainian members of ransomware gangs and their affiliates may have led to the formation of Conti Leaks, a dump of chat logs from the ransomware group. A short-lived Twitter account called @TrickbotLeaks then [doxxed](#) (revealed personal or private information about) alleged members of the Trickbot, Conti, Mazo, Diavol, Ryuk, and Wizard Spiders crime groups.

Among the information to be gleaned from that drama? More evidence that, as many Western researchers have said for years, the Russian Federal Security Service (FSB) is closely connected to a number of ransomware groups, and may even have contracted with those entities for specific Conti incursions.

Alas, none of this internecine conflict led to a significant or long-term decrease in ransomware activity globally. And though 2022 began with multiple arrests by FSB officials of members of both the REvil ransomware-as-a-service group ([in January](#)) and an unnamed carding gang ([in February](#)), even [extraditing](#) a REvil member to the US for trial in early March, by midyear that sort of international crimefighting collaboration seemed unthinkable – and there were signs that REvil, or something pretending to be that service, had already [reawakened](#). And the war goes on.

## Malware economics

While many aspects of the threat landscape have evolved over the past year, perhaps the most significant is the continued development of the cybercriminal economy. That ecosystem has increasingly transformed into an industry unto itself, with a network of supporting services and well-established, professionalized approaches to operations.

Just as information technology companies have shifted to “as-a-service” offerings, so has the cybercrime ecosystem. Access brokers, ransomware, information-stealing malware, malware delivery, and other elements of cybercrime operations have lowered barriers to entry for would-be cybercriminals.

Driving this trend in part are the emerging economics of cybercrime. Criminal marketplaces such as [Genesis](#) make it possible for entry-level cybercriminals to purchase malware and malware deployment services and then in turn sell stolen credentials and other data in bulk. Access brokers use commodity exploits of vulnerable software to gain footholds on hundreds of networks and then sell them to other criminals, often selling the same exploited access multiple times. And ransomware affiliates and other attackers purchase credentials and access to perform higher risk and higher reward criminal activities.

The industrialization of ransomware has allowed for the development of ransomware “affiliates” into more professional operations specializing in exploitation. Using professional offensive-security tools, legitimate administrative and technical support software, malware-as-a-service, and other market-obtained exploits and malware, we’ve seen a convergence by actors around sets of tools, tactics, and practices that can no longer be associated with specific ransomware operations, state-aligned espionage, or other specific motives. These professionalized groups specialize in gaining (or purchasing) access for any motivated actor willing to pay—or, in some cases, multiple actors with multiple motives.

These groups have in many ways mimicked the cloud and web services industry in their business models. Much as the corporate IT realm has adopted the “as-a-service” model for an increasing scope of operations, nearly every aspect of the cybercrime toolkit can be outsourced to crime-as-a-service providers that advertise on underground web boards. We’ll briefly cover nine variations on the theme, and save a tenth for further discussion.

## A naughty nine

**Access-as-a-service:** Access to compromised accounts and systems are sold singly or in bulk through underground services, including remote desktop protocol (RDP) and VPN credentials, accounts, databases, web shells, and exploitable vulnerabilities.

The screenshot shows a dark-themed interface with a sidebar on the left and a main content area on the right. The sidebar contains a logo with the text 'KEEP CALM AND LOVE A HACKER', the name 'Romanians', and 'HDD-drive'. Below this, it says 'Пользователь' and lists statistics: 'Joined: Jun 14, 2022', 'Messages: 35', and 'Reaction scores: 0'. The main content area has a date 'Sep 6, 2022' and several lines of text: 'FRESH 400 RDP'S 50%- VALID RATE (200 RDP'S)', 'Replacement Availble Only in 24 Hours Not more', 'Zoominfo And other things I Didn't checked I don't have time', '200/RDP's', 'Mix Country / Bulk-Selling', '99% Administrator Rights', '90% NO ANTIVIRUS', 'Local / Shares / Neighbor PCs', '80% Asian Country Korea / China / HK / India . etc', 'Workgroup', '10\$ 1 RDP', 'start 2 000\$', 'step \$500', 'Bilts 4 000\$', and 'Garantor will always be accepted here!'. The Sophos X-Ops logo is in the bottom right corner.

Fig. 3. An access broker, seeking a quick sale, touts its wares.

**VPN-RDP / TOP-EU / 5kk**  
By LummA, Tuesday at 08:45 AM in Auctions

**LummaA**  
byte

Posted Tuesday at 08:45 AM

Geo: EU BE Belgium  
Access: VPN - RDP  
Revenue: 5kk  
Activity: Wholesale industry, supply to EU, busy active company  
Rights: DA Admin  
AV: Bit Defender

Paid registration  
● 0  
4 posts  
Joined  
03/05/22 (ID: 126577)  
Activity  
хакинг / hacking

Start: 250\$  
Step: 250\$  
Blitz: 750\$  
PPS: 24 hours

Дам доступ тем кто с репой или с депозитом, остальные через гарант

Fig. 4. An EU company's data on the auction block

**Malware distribution/spreading-as-a-service:** Facilitating the distribution of malware within specific regions or sectors, or even more broadly. In the ads we saw for these services, it's not clear exactly how this is achieved in every case, but possible vectors include watering-hole attacks, exploitation of vulnerabilities, or crossovers with AaaS [access-as-a-service] listings.

★ Spreading your Virus (installs) ★

**ZorosPalace**  
Junior  
Member

01-28-2022, 02:49 PM

Greetings,

Welcome to our new service. We are spreading your viruses/loggers (.exe) all over the world, including USA, EU, CA, AU, NZ, GB.

The virus will be spread by a webmaster.

You can specify which regions you would like to spread your virus. We can do the following regions:

(prices for 1000 downloads)  
-World - 200\$  
-Europe - 1500\$  
-USA - 2000\$  
-CA, AU, NZ, GB - 1200\$

Minimum download volume is 500.  
Maximum download volume we can parse is 20.000 (more can be discussed privately)

We will provide the statistics.

Bulk orders receive good discounts.

We do not load these types of viruses: Lockers, Encryptors, Ransomware

Note for orders: Include the region you would like to spread your virus and direct link to .exe

Fig. 5. A fledgling service offers malware propagation services.

**Phishing-as-a-service:** Threat actors offering end-to-end service for phishing campaigns, including cloned sites, hosting, crafted emails to bypass spam filters, and panels for monitoring results.

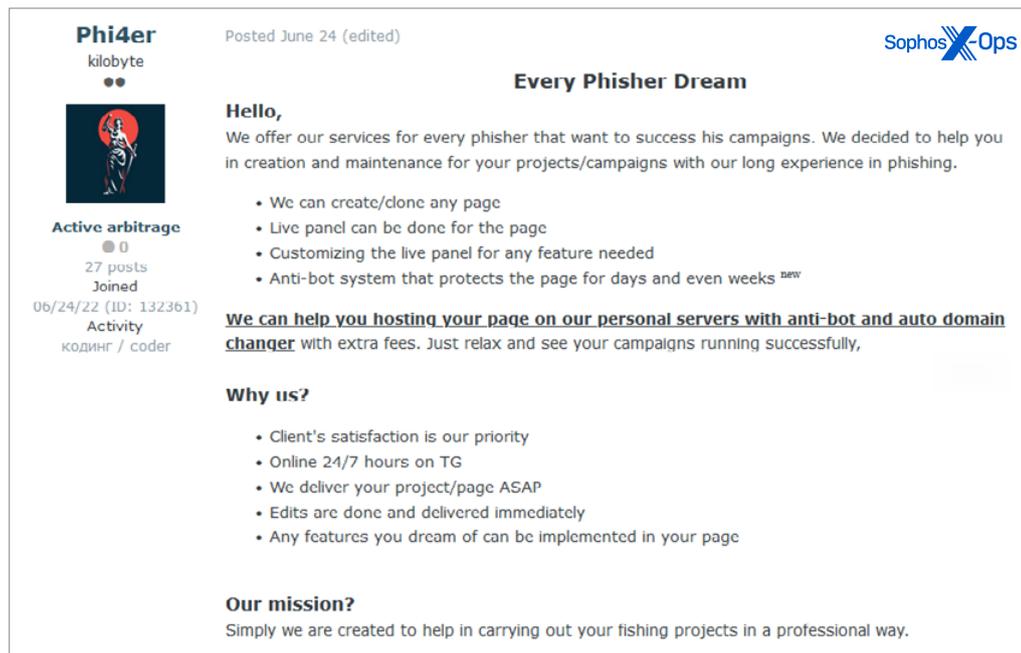


Fig. 6. A suite of phishing services comes with customer-service guarantees.

**OPSEC-as-a-service:** A particularly interesting service, which we saw bundled with Cobalt Strike on a criminal forum. The seller offers to assist buyers by providing an OPSEC service, either a one-off set-up or a monthly subscription, designed to hide Cobalt Strike infections and minimize the risk of detection and attribution.

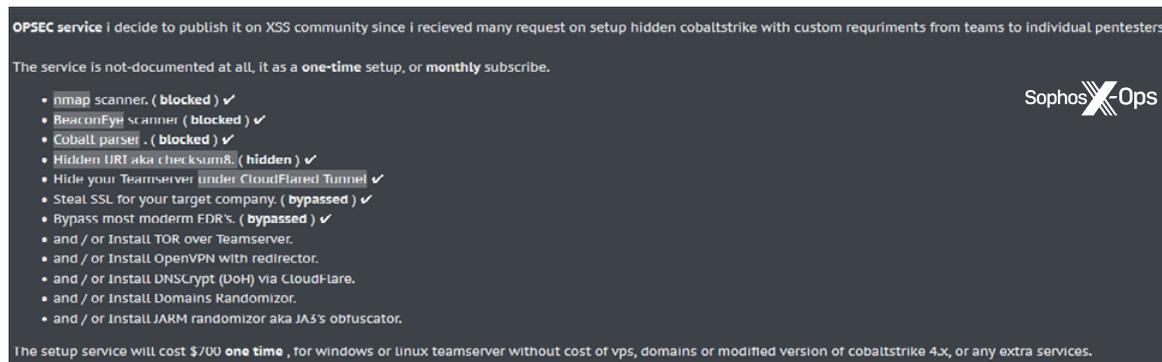


Fig. 7. Specialty service providers help attackers to cover their tracks.

**Crypting-as-a-service:** A common service offered for sale on many forums, crypting-as-a-service is designed to encrypt malware so that it bypasses detection – particularly by Windows Defender and SmartScreen, and by antivirus products to a lesser extent. In the example shown below, the service was offered at \$75 for a one-time purchase, and \$300 for a one-month subscription, which included unlimited use of the service.

**Helium**  
Malware Services



Paid registration  
3  
68 posts  
Joined  
08/16/21 (ID: 119109)  
Activity  
вирусология / malware



Posted 16 hours ago (edited) Report post

Our WD crypting service is one of a kind. You won't have to go through the hassle of finding a reputable crypting service any longer.  
With our exclusive .bat encryption - your executable (.exe) will be transformed into a small, 6-25 kb batch (.bat) file.  
This ensures the best results for manual file distribution.

Using a .bat file has many advantages over the classic .exe file.

- **Guaranteed WD Bypass**
- **Bypass ChromAlert & SmartScreen** (bypasses SmartScreen with non-passworded .zip or .rar file)
- Easy to run and your file will stay undetected for much longer than with a classic .exe
- No need for an EV Signing Certificate compared to regular .exe files

**Features:**

- Adds a **Windows Defender exclusion** for your file when ran on a computer - this way you won't lose connection.
- Loads your executable from an external host straight to the computer when the .bat file is executed.
- Your file will receive a ripped signature for further anti-detection.

Fig. 8. Looking to dodge detection, a specialty service offers to turn .exe files into .bat files.

**Scamming-as-a-service:** We saw a few examples of “scamming kits,” particularly related to cryptocurrency scams, advertised on criminal forums. It wasn't always exactly clear what was being sold, but one listing offered a ready-made “Elon Musk Giveaway BTC Scampage” for \$450. This has been a popular scam since at least 2018, and has done the rounds on [Twitter](#), [Medium](#), and even a [deepfaked video](#).

**Vishing-as-a-service:** A voice phishing (“vishing”) service, whereby a threat actor offered to rent a voice system to receive calls, together with an “AI system” so that the renter could opt to have victims speak to a bot rather than a human.

**Mr.Wizard**  
byte



User  
1  
19 posts  
Joined  
03/17/18 (ID: 86273)  
Activity  
кодинг / coder

Posted August 18 (edited)

Renting a Voice SYSTEM TO RECEIVE CALLS With Live Panel to get CC + OTP.

The victim will call the number then will follow the steps during the calls.

Also there AI system Incase your victim to speak to the bot.

All Language.  
All Accent.

1 Month = \$1500 ( 1 Bank or Service ).

Guarantor Accepted ( Buyer pay the fees )

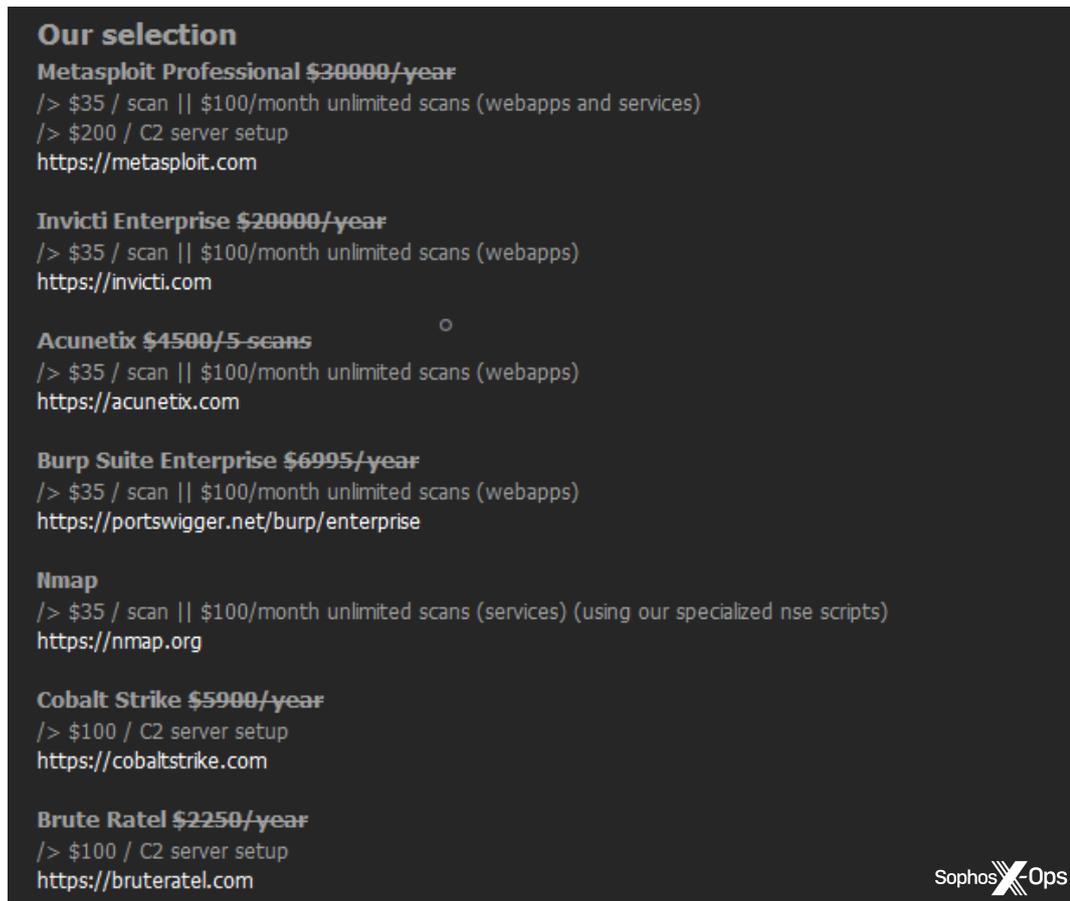
I can customize it to your needs.  
Contact me to show you a demo.



Fig. 9. A vishing-as-a-service offering includes “all language, all accent.”

**Spamming-as-a-service:** An old favorite, but still prevalent on criminal forums, spamming-as-a-service offers bulk spamming through a variety of mechanisms, including SMS and email. In some cases the threat actor offers to set up the entire infrastructure from scratch; in others, they operate the infrastructure and use it to send custom spam messages.

**Scanning-as-a-service:** Finally, a particularly interesting service offered on a criminal forum, which offered users access to a suite of legitimate commercial tools – including Metasploit, Invicti, Burp Suite, Cobalt Strike, and Brute Ratel – in order to find (and, presumably, exploit) vulnerabilities. As we see in Figure 10, prices were heavily discounted. All the infrastructure is apparently created and maintained by the seller, who claims elsewhere that “you just have to wait for the scan result in the mail.”



**Our selection**

**Metasploit Professional ~~\$30000/year~~**  
 /> \$35 / scan || \$100/month unlimited scans (webapps and services)  
 /> \$200 / C2 server setup  
<https://metasploit.com>

**Invicti Enterprise ~~\$20000/year~~**  
 /> \$35 / scan || \$100/month unlimited scans (webapps)  
<https://invicti.com>

**Acunetix ~~\$4500/5-scans~~**  
 /> \$35 / scan || \$100/month unlimited scans (webapps)  
<https://acunetix.com>

**Burp Suite Enterprise ~~\$6995/year~~**  
 /> \$35 / scan || \$100/month unlimited scans (webapps)  
<https://portswigger.net/burp/enterprise>

**Nmap**  
 /> \$35 / scan || \$100/month unlimited scans (services) (using our specialized nse scripts)  
<https://nmap.org>

**Cobalt Strike ~~\$5900/year~~**  
 /> \$100 / C2 server setup  
<https://cobaltstrike.com>

**Brute Ratel ~~\$2250/year~~**  
 /> \$100 / C2 server setup  
<https://bruteratel.com>

Sophos  Ops

Fig. 10. A scanning-as-a-service provider lists access to various suites of popular commercial tools.

## Maturing from 133t to slick

As the 'as-a-service' industry grows, and criminal marketplaces become increasingly commodified, so the look and feel of those marketplaces changes. On one prominent forum, for example, users can pay for advertisement space, and display animated banner ads to the forum's thousands of users. Note that one of the ads in the example below is for the aforementioned Genesis, a popular marketplace [that we've covered previously](#).

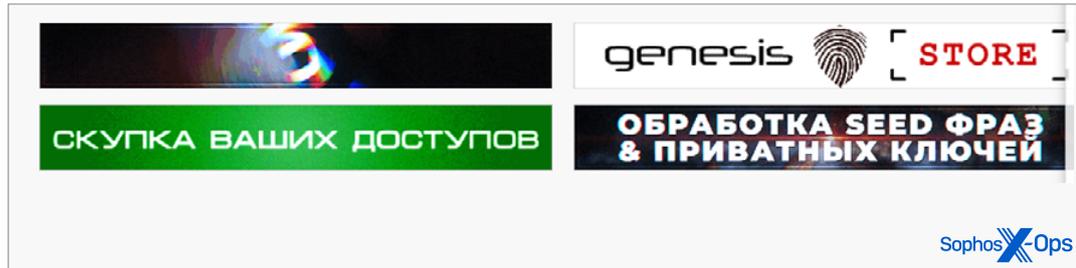


Fig. 11. A criminal forum sports advertisements for a variety of marketplaces and services.

Threat actors are also becoming more aware of the benefits of professional graphic design and layout. Whereas a few years ago, malware and service listings were typically simple, text-heavy posts containing lists of features and capabilities, today's offerings are often accompanied by eye-catching imagery designed to give products an air of professionalism, brand differentiation, and legitimacy.

**Zed Point**

**Europol & Interpol**  
dossier | wanted list | negative

Searching :

- + Flights / Travel
- + The fact of having a Residence Permit
- + Availability of real estate in the euro zone
- + Bank accounts / account balance
- + Vehicles (auto, motorcycle, air)
- + Search and selection of data (passport, ID, DL)

and much more

**Around the world !**  
Call billing | Locate a phone | Mobile movement | Set the phone number by IMEI

**Весь мир!**  
Детализация звонков | Вспышка | Передвижение абонента | Установим номер по IMEI

Европол / Интерпол  
Анкеты | досье | розыск | негатив

Установим : Наличие гражданства | Перелеты / Передвижения | Факт наличия Вида на Жительство | Наличие недвижимости в евро зоне | Банковские счета / остаток по счету  
Транспортные средства ( авто, мото, авиа )  
Поиск и подбор данных ( passport . ID .DL )

Fig. 12. The Zed Point service purports to provide information that could facilitate identity alteration or theft.

Fig. 13. NoCry gathers and maintains access to stolen session cookies.

Products and services aren't the only thing advertised on marketplaces. As the criminal economy continues to grow and professionalize, job offers and recruitment posts have become increasingly common. Several prominent marketplaces have dedicated help-wanted pages, both for those seeking employment (usually as "pentesters," often a euphemism for ransomware affiliates) and those recruiting staff.

▲  
0  
▼

**[JOB - BTC/XMR] I operate dozens of phishing websites of all kinds. Looking for some "marketers" who can bring people in for a 50/50 split**  
 by /u/carderman · 1 week ago in /d/Jobs4Crypto

Like the title states, I've got a bunch of different custom-built phishing websites, ranging from fake darknet markets, fake crypto exchanges, email templates with fake giveaways & crypto promos, fake carding sites, simple landing pages, and so on.

I'm looking for someone or someones who'd like to bring people in, via spamming, social engineering, whatever method works for you... and if they take the bait, we split their generous donations 50/50.

I've had some of these up for anywhere from over a year to some I just created this week. These sites bring in a decent chunk of change as they are, but I've never been opposed to more money.

If interested in getting started, or simply learning more about them, just DM me and I can send you some links and you can choose which ones you think you might be able to do something with.

We can keep track of which ones are yours using a coupon code or custom "referral" url. I have a couple ideas for making sure we're on the same page when it comes to keeping track of which "sales" are yours. I'm keen to ensure you're compensated fairly for the hits you bring in because that's just good business - this shit is already passive AF and basically free money for me at the end of the day. But if you can bring in more free money then I'm more than happy to keep you happy if that means you'll keep selling.

Hell, if you're really good, I'd be more than happy to give you the lions share.

Let's make some money, ladies!

Sophos X-Ops

Fig. 14. Alliances between entities with differing skill sets allow for increased efficiency.

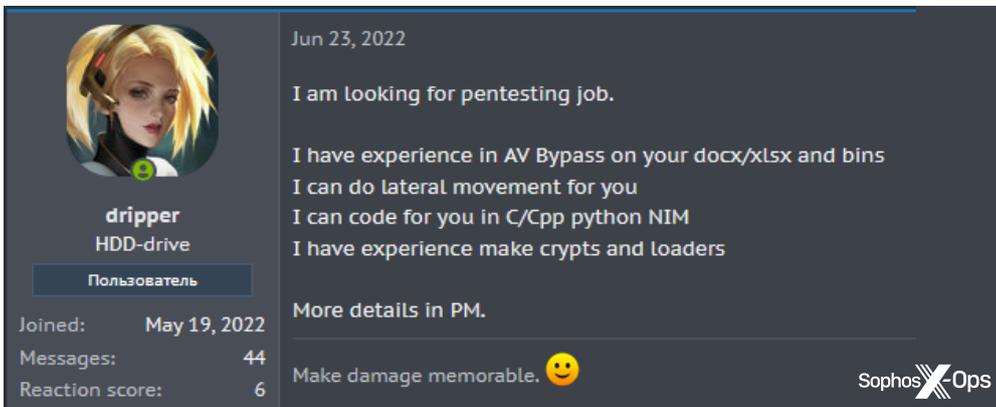


Fig. 15. An experienced “pentester” seeks work with an established entity.

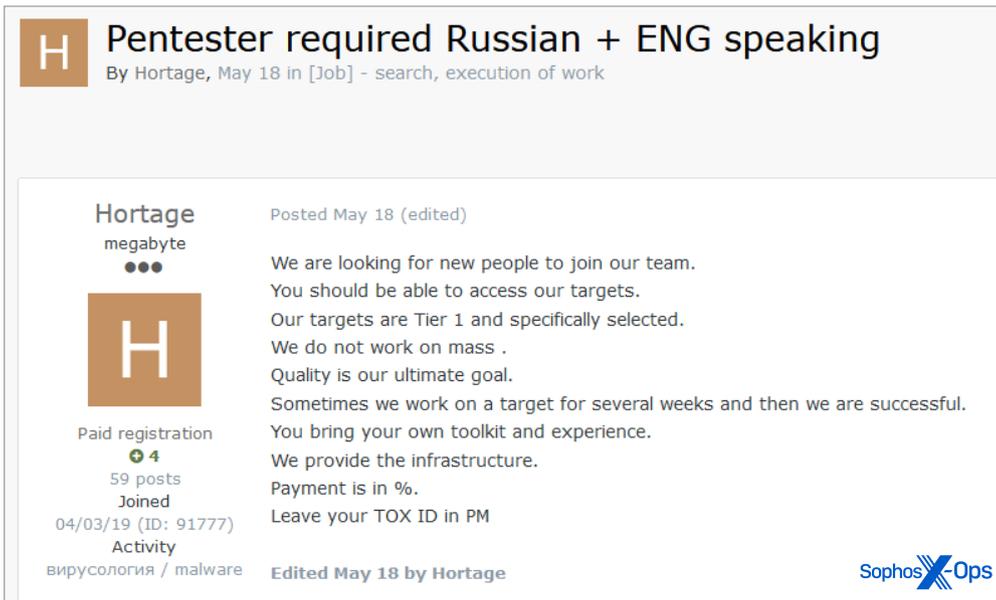


Fig. 16. An established criminal gang seeks additional members.

## Infostealers

Information-stealing services are part of the supporting infrastructure of the malware economy – akin to, but larger than, the “[bad thing]-as-a-service” offerings we just enumerated. Thanks to malware-as-a-service and malware-deployment-as-a-service offerings, would-be cybercriminals can get started with a small investment and not much in the way of skills other than the ability to log into web control panels, and to gain access to credentials marketplaces.

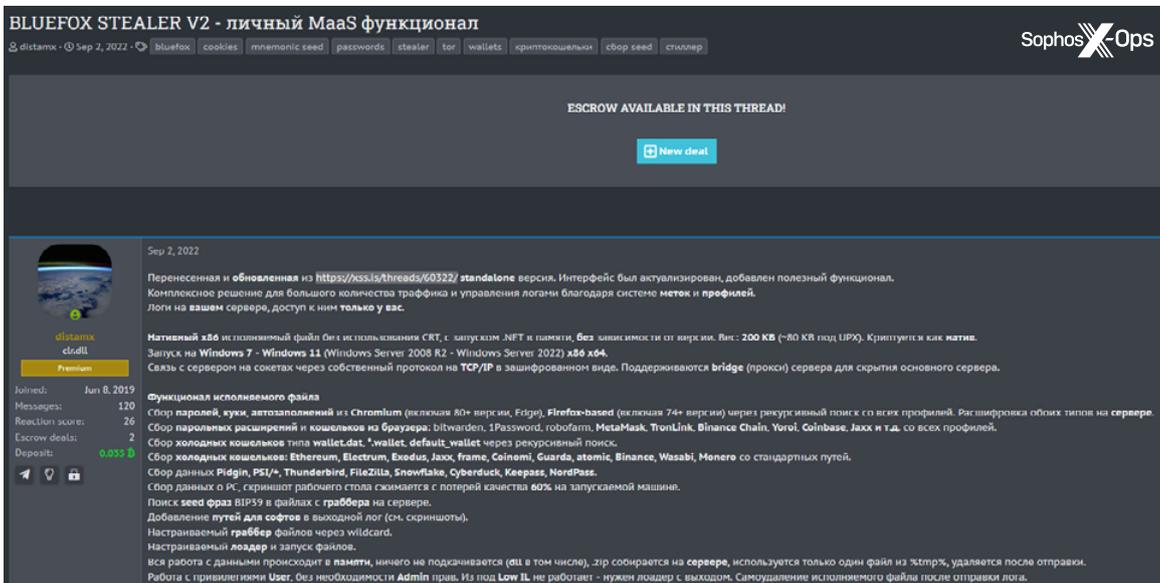


Fig. 17. Information-stealing services thrive in the specialization-friendly cybercrime ecosystem.

The entrepreneurial cybercriminal can then resell stolen credentials in a number of underground marketplaces. In some cases, these credentials are just information bycatch, harvested with stolen cryptocurrency transactions and other methods of malware monetization.

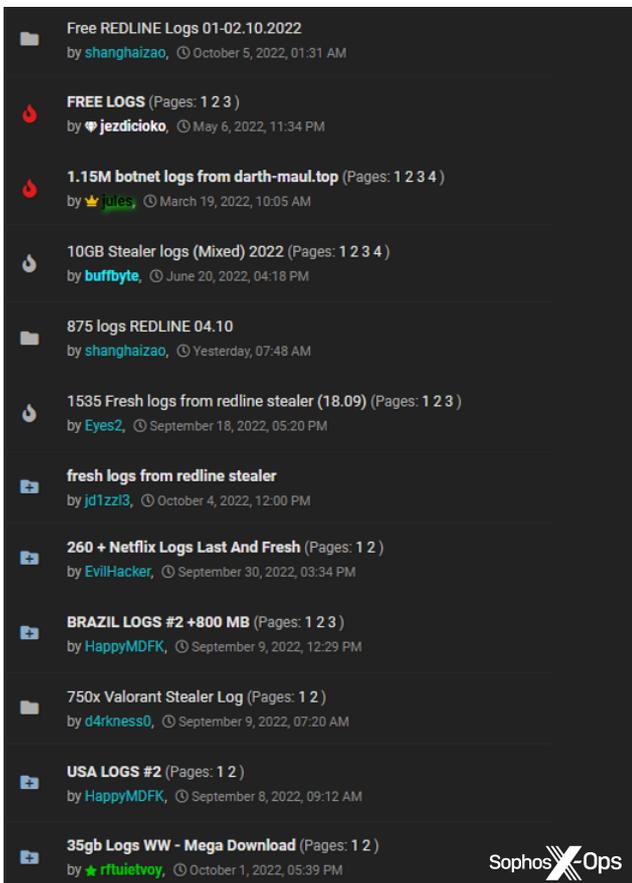


Fig. 18. Stolen "logs," including passwords and other credentials, for sale

Finally, the infostealer ecosystem is very aware that defenders are interested in its doings – and, true to form, sees an opportunity for profit. One underground forum, XSS, recently [sought](#) to monetize white-hat efforts to scrape their forums by offering a \$2000 annual subscription for unimpeded data-collection access.

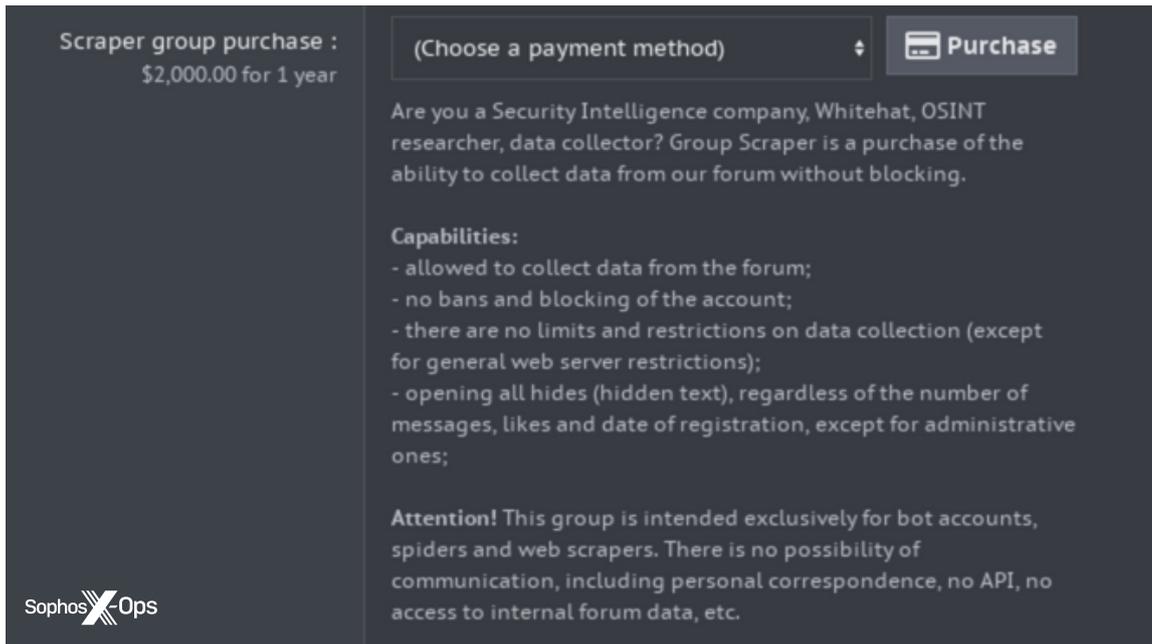


Fig. 19. A forum offers paid access to blue-hat scrapers attempting to keep an eye on criminal activities. (The second image provides the text translated from Russian to English.)

Information-stealing malware is a broad label. It includes various malware types touched on elsewhere in this report, including remote access tools (RATs), keyloggers, cryptocurrency-focused “clippers,” and other malware that grabs [credentials](#), browser cookies, cryptocurrency transactions, or any other data that can be quickly stolen and sold or reused for other malicious purposes.

Information stealers provided the Slack cookies used by the Lapsus\$ gang to gain access to Electronic Arts’ corporate network in 2021. They have been likewise implicated in other, more recent malicious activities that have leveraged stolen session tokens for web applications into more persistent and pervasive access—ranging from business email compromise to ransomware attacks.

### Information stealers tracked by percentage of unique machines

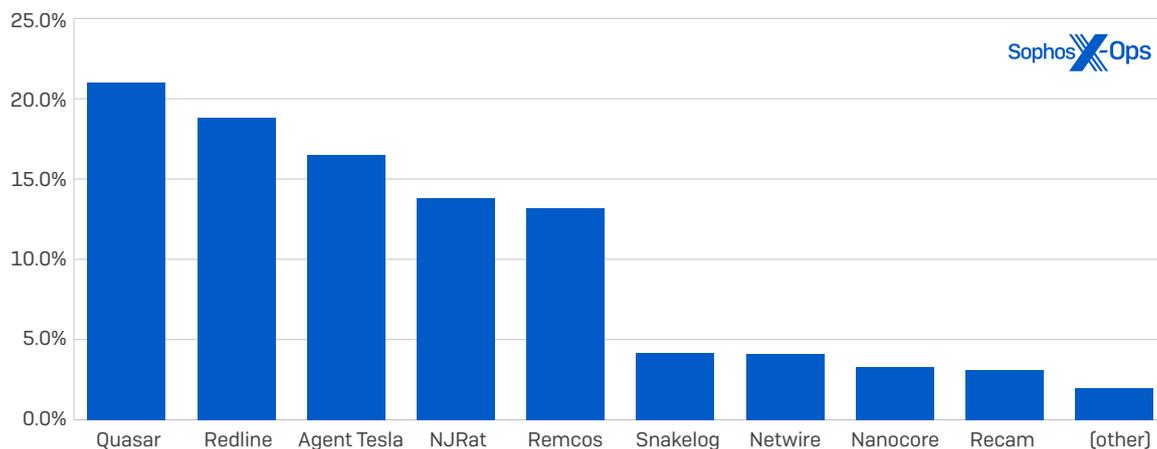


Fig. 20. Quasar, Redline, and Agent Tesla account for the lion’s share of discovered information-stealing malware, with Quasar found on over one-fifth of infected machines over a six-month period.

Those interested in the infostealer space may note the absence in the figure above of the notorious Raccoon Stealer. After entering the scene in 2019, the Ukraine-based, Windows-focused malware temporarily disappeared from the landscape in early 2022 after action by the FBI working with Dutch and Italian authorities, only to return under new management as the year wore on. Development of a new version launched in June, and the completed new version was announced on the authors' Telegram channel in September. However, despite widespread awareness of the relaunch, we have so far seen very few recent instances of the new Raccoon Stealer. In late October, the US Department of Justice [unsealed](#) an indictment charging a Ukrainian national currently in Dutch custody with conspiracy to operate the service.

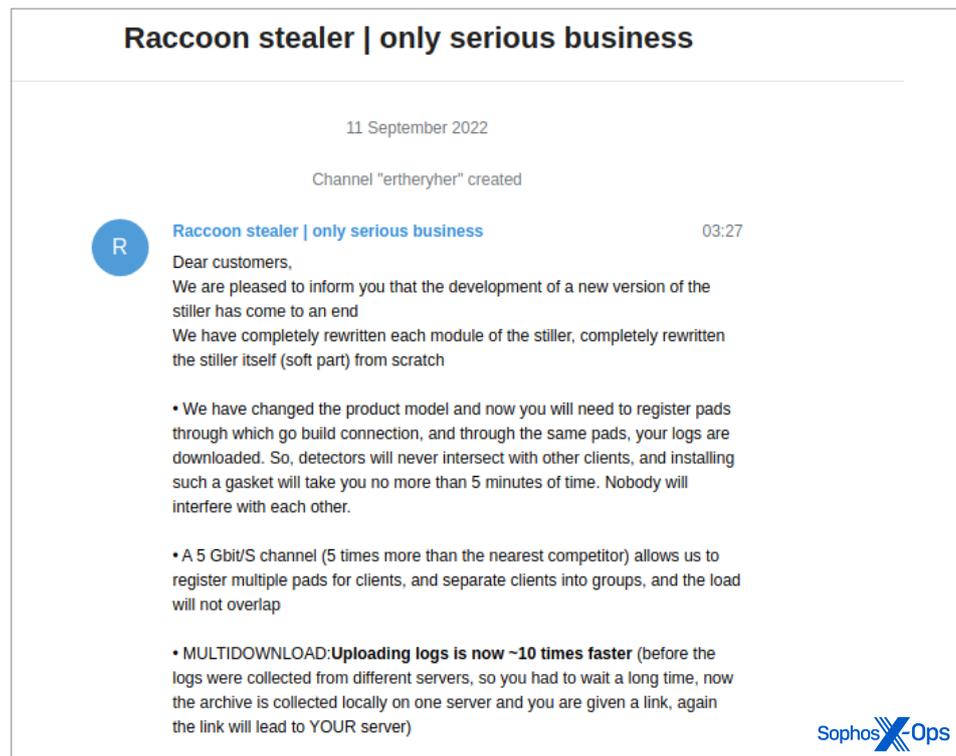


Fig. 21. Raccoon Stealer announced its latest version on the group's Telegram channel in September.

Information stealers propagate through a variety of channels. One of the most common is social engineering-based downloader-as-a-service offerings that lure users into grabbing archive files or disk images purporting to contain legitimate software installers, usually advertised as "cracked" versions bypassing licensing schemes. The downloads also carry installers for multiple malware packages. These download sites use search engine optimization techniques to raise them to the top of any search for "cracked" software. Other paid distribution happens through botnets such as Emotet or Qakbot/Qbot.

Some stealers, such as Agent Tesla, usually use more targeted approaches, devising malicious emails targeted to a specific set of victims. These contain attachments disguised as urgent documents, which are actually malware installers.

But information stealers can be deployed in even more targeted ways. Sophos has tracked incidents where intruders on a network used a backdoor deployed via Cobalt Strike to launch cookie-stealing malware and other credential-stealing malware from within the network. Efforts were made to harvest browser cookies from systems that included a server; these could then be used to gain access as legitimate users to the organization's web-based resources for further lateral movement.

Sophos has deployed a number of measures to block information stealers, and has added cookie theft protection to prevent information-stealing efforts from harvesting session cookies.

## Ransomware evolution

While there has been some disruption of ransomware groups over the past year thanks to (among other reasons) geopolitical unrest and the occasional prosecution, new groups have arisen from the old, and ransomware activity remains one of the most pervasive cybercrime threats to organizations. Ransomware operators continue to evolve their activities and mechanisms, both to evade detection and to incorporate novel techniques.

Some ransomware groups have embraced the use of new programming languages in an effort to make detection more difficult, to make the ransomware executable more easily compiled to run under different operating systems or platforms, or simply because the people developing malware payloads bring those skills and tools to the effort. The Rust programming language has been adopted by the developers of BlackCat and Hive ransomware, while BlackByte's malware is written with Go (aka GoLang).

The most prevalent single ransomware seen in Sophos Rapid Response engagements during the first ten months of 2022 was LockBit, followed closely by BlackCat and Phobos. (We note, however, that "other" accounted for over one-fifth of the families noted, indicating that the ransomware landscape is by no means limited to just a few high-profile families.) The distribution is likely fairly close to the actual overall distribution of ransomware attacks in the world overall.

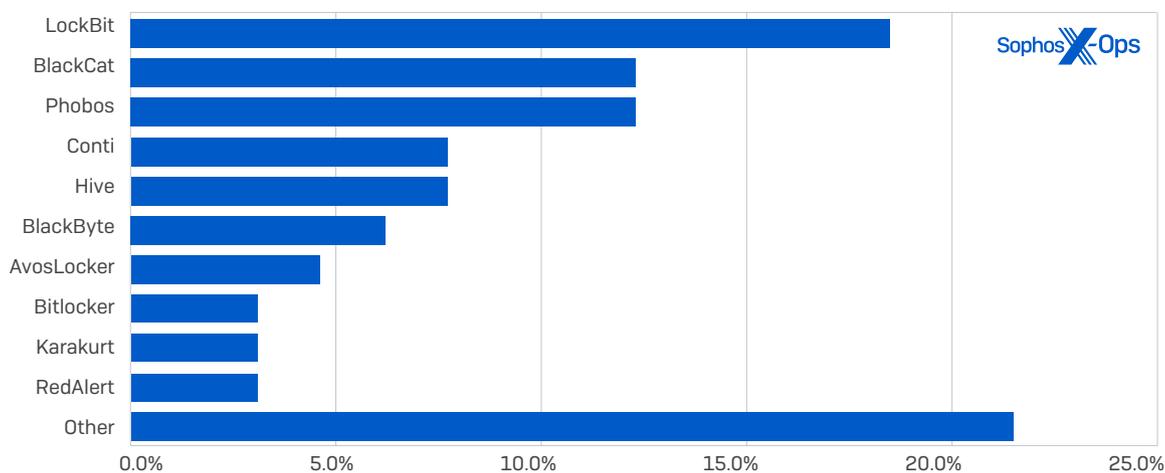


Fig. 22. High-profile entities such as LockBit, BlackCat, and Phobos are common, but the Response landscape varies broadly.

As well as diversifying the languages used, ransomware has also switched up its targeting, no longer focusing solely on Windows. RedAlert, or N13V, [encrypts both Windows and Linux ESXi servers](#), as does [Luna](#) (another Rust-based ransomware strain). But it's not just the second-string players: researchers spotted a [Linux-ESXi variant of LockBit](#) at the start of the year. Shifts in targeted platforms mean more opportunities for threat actors – a wider attack surface, more pressure on victims, and potentially less risk of detection, as the majority of anti-ransomware measures focus on Windows. We'll look more closely at the threat landscapes for Linux, Mac, and mobile platforms later in this report.

We've also seen some developments in how ransomware is deployed on compromised systems. Two ransomware incidents our SophosLabs team analyzed earlier in the year – one involving Darkside, the other Exx ransomware – involved the abuse of otherwise benign applications for [DLL sideloading](#). In the Darkside case, the threat actor used a clean antivirus utility program; with Exx, it was a Google updater. After years of popularity with certain niche-target attackers, DLL sideloading is fast becoming a popular tactic with threat actors, as it can allow them to evade detection by executing malicious payloads under the guise of legitimate processes.

As far as delivering and spreading ransomware goes, threat actors continue to improvise and adapt. We've seen [Impacket](#), a collection of open-source Python modules for working with network protocols, being abused for lateral movement on compromised networks. Impacket's toolset includes remote execution capabilities, credential sniffing and dumping scripts, exploits for known vulnerabilities, and enumeration

modules – making it a very attractive package for ransomware actors. It’s intended to be a legitimate security testing tool but, much like Metasploit and Cobalt Strike, its features and capabilities attract less-savory customers. On the same note, we’ve also seen Brute Ratel being used for payload delivery, as noted above. The rise of attacker abuse of legitimate security tools (“dual use”) requires that defenders be scrupulously aware of what’s operating on their network (and why), and who’s got rights to do so.

Ransomware groups also seem to be exploring more general opportunities to diversify their operations. A key example is the growth of leak sites, where threat actors post details of their victims. Traditionally, the model has been fairly simple: if organizations pay, their data isn’t published on the leak site. If they don’t, it is. But this year has seen some interesting developments in that space.

As one of the biggest ransomware groups, LockBit has been ahead of the pack in this regard. Its new leak site, to go along with the new version of its ransomware, [LockBit 3.0](#) (also known as LockBit Black, possibly because many of its capabilities and a significant portion of its code appear to be based on BlackMatter ransomware) contains some novel features. For instance, one money-maker devised by the group is to offer visitors, or the victim, the chance to destroy or purchase the stolen data, or to extend the timer counting down to publication.

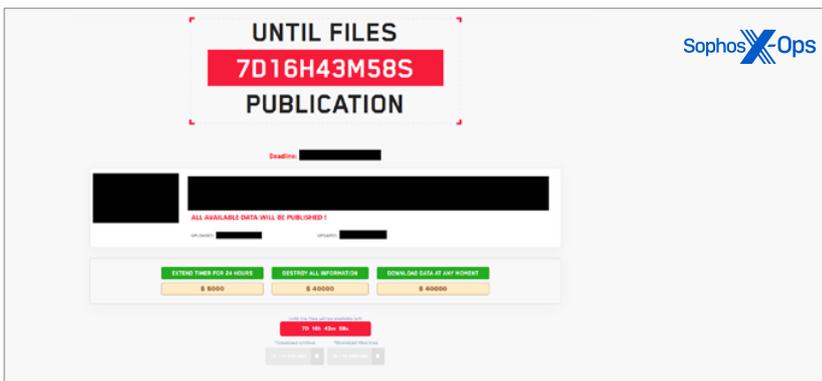


Fig. 23. Options to extend the ransomware timer, or to download (or destroy) the data, are presented to a LockBit victim.

Other ransomware groups, such as Karakurt and AvosLocker, have jumped on this bandwagon, facilitating auctions for stolen data. Still others, such as Snatch, are promising to move their leaks to a subscription mode. Some sites offer a twist on post-disclosure visibility; if a victim pays, not only is the information not made public, but the fact of the breach itself is not made public (or, if it the victim’s condition has been publicized to leak sites, that mention is removed) – possibly making the victim complicit in concealing activity that is in many nations required to be reported to regulators.

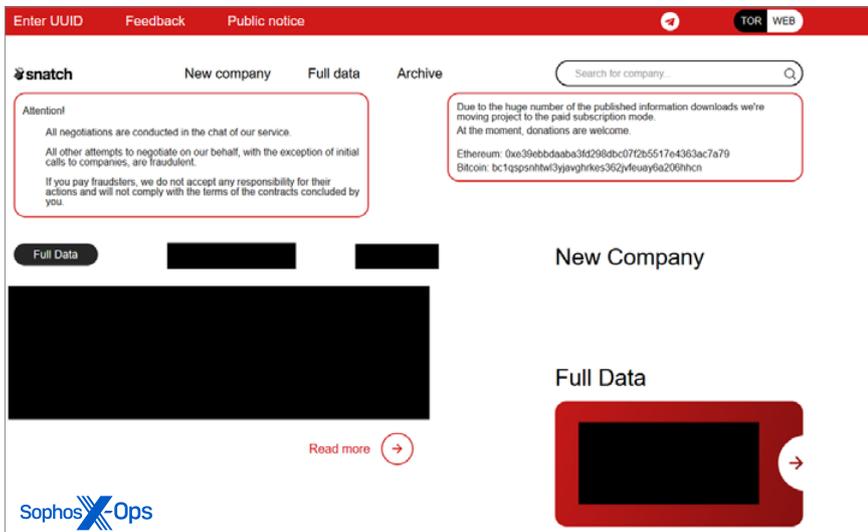


Fig. 24. The Snatch ransomware moves to a subscription model.

But LockBit has taken it one step further, innovating not only with regard to its core product, but also in its interactions and position within the criminal community. Its new leak site, for instance, offers a bug bounty, with remuneration “from \$1000 to \$1 million” offered for a variety of activities that would, ultimately, strengthen the service:

- Private disclosure of bugs in its website or malware
- A successful dox of the head of LockBit’s own affiliate program, with details as to how they did it, presumably so that LockBit can harden its OPSEC; this is the million-dollar award
- Vulnerabilities in the TOX messenger (an instant-messaging package heavily used by threat actors)
- Ideas on improving LockBit ransomware
- Information-disclosure vulnerabilities in its onion domain or other aspects of the TOR network

LockBit is not the first threat actor to offer bug bounties – back in November 2021, All World Cards, a prominent carding group active on several Russian-language cybercrime forums, offered rewards of up to \$10,000 for vulnerabilities found in its store. And it probably won’t be the last. It’s an effective method of crowdsourcing penetration testing and vulnerability assessments, while ensuring that any findings stay between the researcher and the threat actor.

Nov 9, 2021

We are opening the bug bounty program!  
List of vulnerability types and rewards:

**Low risk bug**

- Bug with displaying items
- Insufficient Authentication
- Session Prediction
- Directory Indexing
- Information Leakage

**Reward: 10-100 usd**

**Medium risk bug**

- Weak Password Recovery Validation
- Insufficient Authorization
- Content Spoofing
- XSS
- HTTP Response Splitting
- Predictable Resource Location
- Sensitive Data Exposure
- Path Traversal

**Reward: 100-500 usd**

**High risk bug**

- Abuse of Functionality

**Reward: 500-1000 usd**

**Critical risk bug**

- SQL Injection
- RCE
- File Inclusion (read, execute file)

**Reward: 1000-10000 usd**

**If you want to inform us about the vulnerability, then you need to:**

- 1) Type of vulnerability and its description
- 2) Instructions on how to reproduce this problem
- 3) Video demonstration of the vulnerability (fully replaying it)
- 4) Your login to our store.

Sophos X-Ops

Fig. 25. All World Cards unveiled a modest bug-bounty program in late 2021.

Finally, we noted a couple of lesser-known ransomware or leak groups which, unlike some of their more famous cousins, seem to be politically motivated. First up is a leak site dedicated to sharing materials from breaches of Ukrainian citizens and government organizations, although it’s not clear where the data originates and if ransomware is involved.

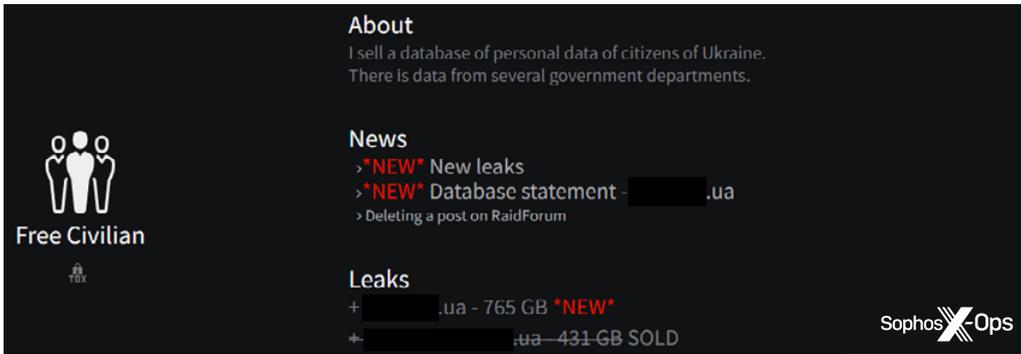


Fig. 26. Ukrainian civilians targeted by nation-focused attacker

There's also a group known as Moses Staff, which [appears to target Israeli organizations](#) with ransomware-like tactics without actually demanding a ransom.

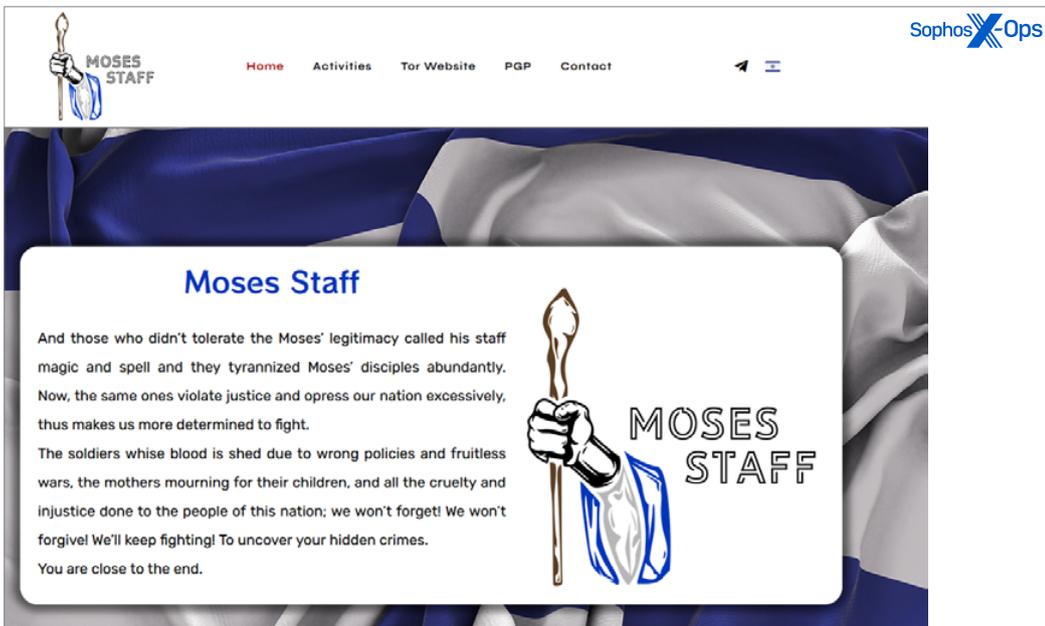


Fig. 27. Anti-Israel group uses ransomware-like tactics to harass

## Attack tooling

For most defenders, the “who” of attacks is less immediately actionable than the “how.” In this section, we’ll look at ways in which attackers are currently subverting offensive security tools for their own purposes. Pen-test tools are an obvious candidate for abuse, but they are not the only legitimate security tools being undermined; we’ll briefly survey other techniques including the use of otherwise legitimate remote-access tools (RATs). After that, we’ll turn our attention to the increase in “LOLBins” – a technique that abuses binaries already present on targeted systems – and to a recent upswing in attackers using otherwise legitimate third-party drivers and DLLs to sneak malicious code past defenses. Finally, we’ll spend some time on two species of malware we found especially interesting in 2022: ransomware that targets endpoint-security upgrades, and “miner” software that steals victims’ resources to indulge in cryptocurrency creation. We’ll close our report with spotlights on the Linux, Mac, and mobile threat landscapes.

## Turning offensive security tools to bad ends

The misapplication of offensive security tools – software intended to be used by information security teams to simulate active attacks – is common in many ransomware campaigns. As we noted last year, pirated copies of the Cobalt Strike commercial penetration testing tool have increasingly been used by adversaries such as ransomware affiliates. Open-source tools developed by the offensive security community – such as the Mimikatz credential harvesting tool (versions of which account for roughly two-fifths of unique attack-tool detections in Sophos telemetry), other PowerShell-based exploitation tools such as PowerSploit, and “Meterpreter” components connected to the partially open-source Metasploit exploitation platform – remain the largest component of overall attack tool detections.

But pirated copies of commercial offensive-security tools have become a standard part of more complex and professional attacks. As documented above, some groups advertise to hire people with skills in those tools. And pirated copies of Cobalt Strike and the commercial version of Metasploit are now so common that links to free copies are frequently posted on underground sites (though some may in fact be malware).

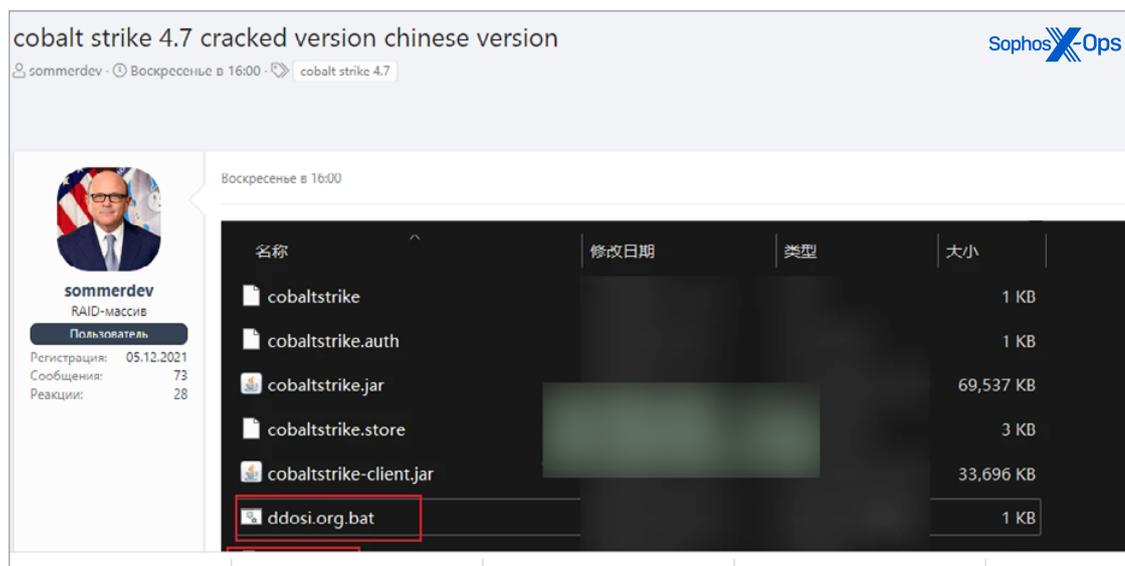


Fig. 28. A Chinese-language version of Cobalt Strike 4.7 is cracked and resold.

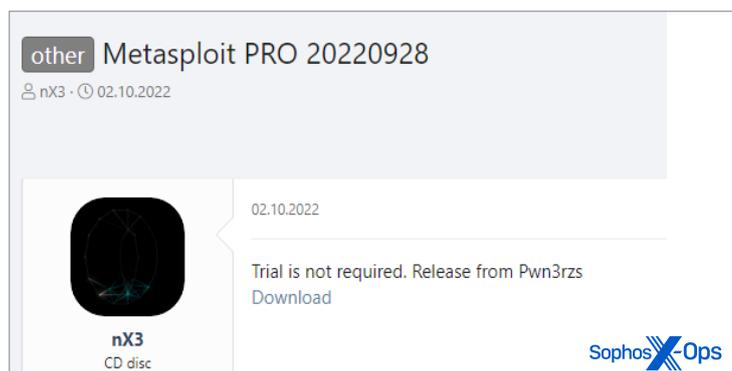


Fig. 29. The paid version of Metasploit is pirated and offered for download.

Cobalt Strike played a role in 47 percent of the customer incidents handled by Sophos’ Rapid Response team during the first three quarters of 2022. The vast majority of these were ransomware-related, or were “pre-ransomware” activity in which threat actors were detected using techniques, tools, and practices associated with impending ransomware attacks. But Cobalt Strike has also been observed as part of state-oriented attacks, such as the 2020 SolarWinds campaign and in attacks on targets in Ukraine by Russia-aligned actors.

On its own, Cobalt Strike has accounted for eight percent of all unique detections for attack tools. In addition, its communication protocol has been rolled into other tools developed by attackers. TurtleLoader, for example, has versions that connect to their command-and-control (C2) network via either the Metasploit or Cobalt Strike connection protocol. Such multi-tool players pose interesting challenges for defenders, especially as different layers of defense are engaged to protect against attacks.

And there is always more to watch for. At the time of this writing, for instance, we have seen attacks involving Brute Ratel climb in the wake of that toolkit's new availability to attackers; when we went to press, Brute Ratel detections were barely a blip on the radar, turning up in less than one percent of our in-memory detections. That will almost definitely change in 2023 as cracks for the product proliferate.

Notable attack tool detections (unique machines over 6-month sample period)		
Attack tool	Percentage of machines infected	Notes
Mimikatz	24.7%	Open-source post-exploitation credential-dump utility
Apteryx	14.5%	A compiled version of Mimikatz
PowerSploit suite	11.7%	Open source; out of official support since August 2020
SrpSuite	8.3%	Open-source PowerShell Suite by FuzzySecurity
Cobalt Strike	8.0%	Proprietary software, often pirated / cracked
Meterpreter	7.8%	Open-source Metasploit attack payload; commercial support available
Nishang	6.8%	Framework and scripts/payloads for use with PowerShell
TheFatRat	6.2%	Open-source Metasploit backdoor / payload automation
TurtleLoader	5.4%	Backdoor, usually seen in conjunction with Metasploit or Cobalt Strike
JMeter	5.1%	Java-based Metasploit
Juicy Potato	5.0%	Open-source BITS exploit (privilege escalation tool)
winPEAS	4.8%	Privilege-escalation and information-stealing scripts
Swrort	4.6%	Metasploit-based backdoor
Empire	4.5%	Open-source post-exploitation framework; merger of PowerShell Empire and Python EmPyre; out of official support since July 2019

Fig. 30: The percentage of infected machines analyzed by Sophos on which the named tool was present, along with further information on some tools; data drawn from a six-month period (April-September 2022) and tools detected on fewer than 4.5 percent of unique machines are omitted for space.



Until September 2022, Brute Ratel's developer claimed to have tight control over access to the tool through licensing provisions. Still, actors associated with the Conti ransomware ring appear to have created fake companies to purchase the platform, and there has been at least one case of a license being leaked by an employee of a legitimate customer. As of September, pirated copies of a recent release of Brute Ratel have become widely available through underground marketplaces.

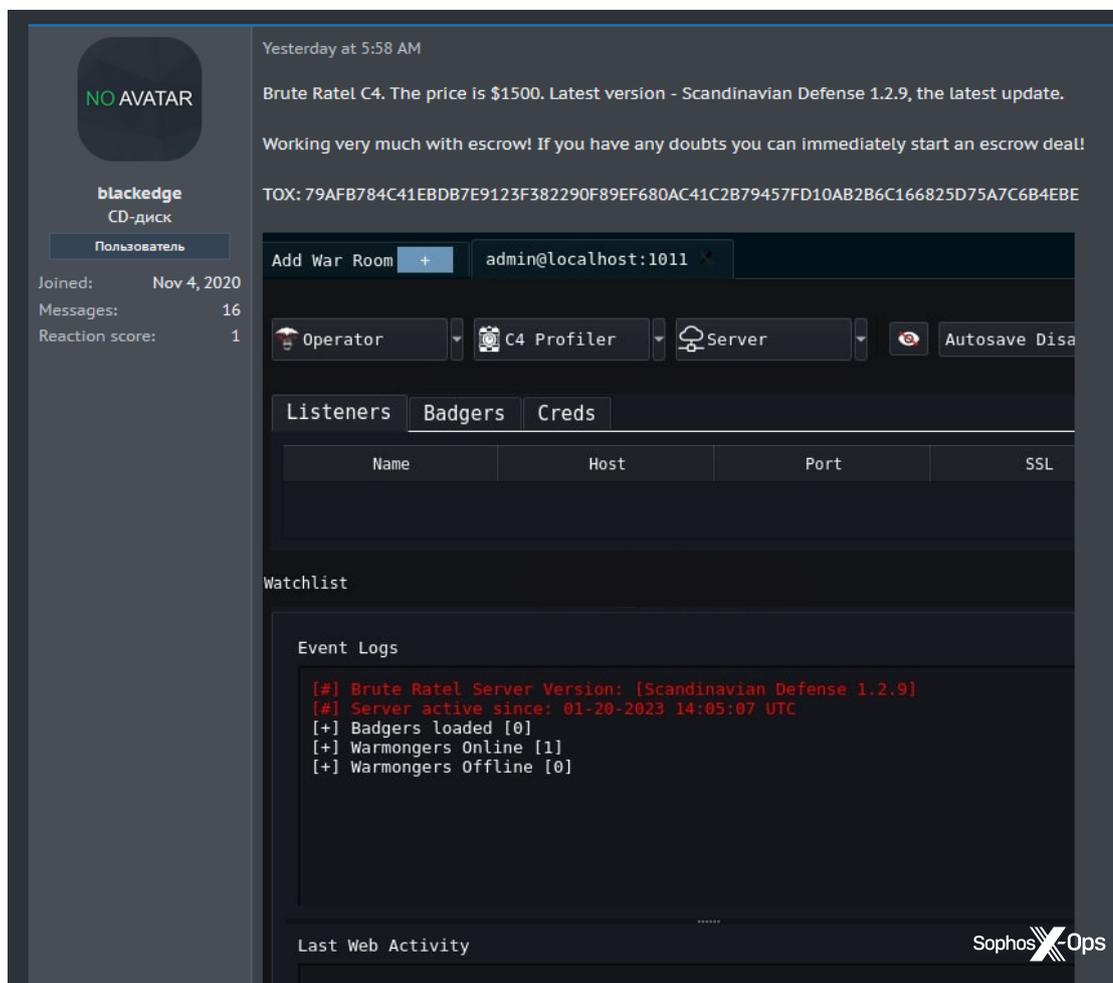


Fig. 31. A cracked version of Brute Ratel debuts underground.

So far, we have documented a smattering of attacks associated with Brute Ratel components. During an incident triage by Sophos MDR, we saw attackers first trying to use Cobalt Strike; when Cobalt Strike was detected and blocked, the adversaries then tried to deploy Brute Ratel – which was also blocked.

But more incidents are highly likely. Perhaps as a result of the wider availability of Brute Ratel, recent research has found Brute Ratel agents being spread by [Qakbot](#), much in the way Cobalt Strike beacons have been spread in the past.

## Other abused security tools

Brute Ratel isn't special in terms of being "repurposed" with ill intent: Threat actors are also offering a number of other legitimate security tools for sale on criminal marketplaces. Examples include Core Impact, a penetration testing framework; Nexpose, a vulnerability scanner; VirusTotal Enterprise; and Carbon Black, an endpoint protection platform.

**VirusTotal Enterprise(Downloader)**  
by mbrk256 - Wednesday September 28, 2022 at 12:48 PM

Sophos X Ops

September 28, 2022, 12:40 PM (This post was last modified: September 28, 2022, 02:31 PM by mbrk256)

I'm selling software that provides VirusTotal Enterprise with an annual fee of \$10,000.

You can download any file in virustotal you want using this software.

Using the software is quite simple. You just need the virustotal scan result link.

Usage Video:

**virustotal-enterprise**  
Powered by dailymotion

**Pricing:**  
\$400 annual license  
\$1,200 unlimited license  
\$6,000 exploit

**Contact for purchase:**  
Telegram: @mbrk256

It has support for Windows, Linux and MacOS.  
**Exclusive to the Breached Forum: 3 days license free to the first person who posts in the thread.**

PM Find

Fig. 32. VirusTotal Enterprise targeted by malicious data-scrappers

Threat-actor use cases for these perfectly legitimate tools vary; they can dissect EDR and endpoint protection platforms to test for vulnerabilities and evasion tactics, automate vulnerability scanning and exploitation with penetration testing and exploit frameworks, and obtain malware samples and counterintelligence through tools such as VirusTotal.

## Dual-use RATs

In the increasingly large array of misappropriated or simply abused security tools in the threat landscape, special mention should be made of remote-access tools. The frequency with which these legitimate tools are turned to illegitimate ends – a toxic example of “dual use” – requires that defenders keep a constant watch for signs of abuse and questionable behavior.

Remote-access tools are used to establish a persistent connection to compromised systems from which to stage attacks. Some of the more prominent remote-access tools include:

- NetSupport Manager [NetSupport]
- TeamViewer Remote Access [TeamViewer]
- ConnectWise Control / Screenconnect Remote Access [ConnectWise]
- AnyDesk [AnyDesk Software]
- Atera [Atera Networks]
- Radmin [Famatech]
- Remote Utilities [Remote Utilities]
- Action1 RMM [Action1]

These tools may be deployed by attackers themselves, or by access brokers selling persistent access to compromised networks. Some cybercriminals openly solicit for victim access through these tools on underground websites:

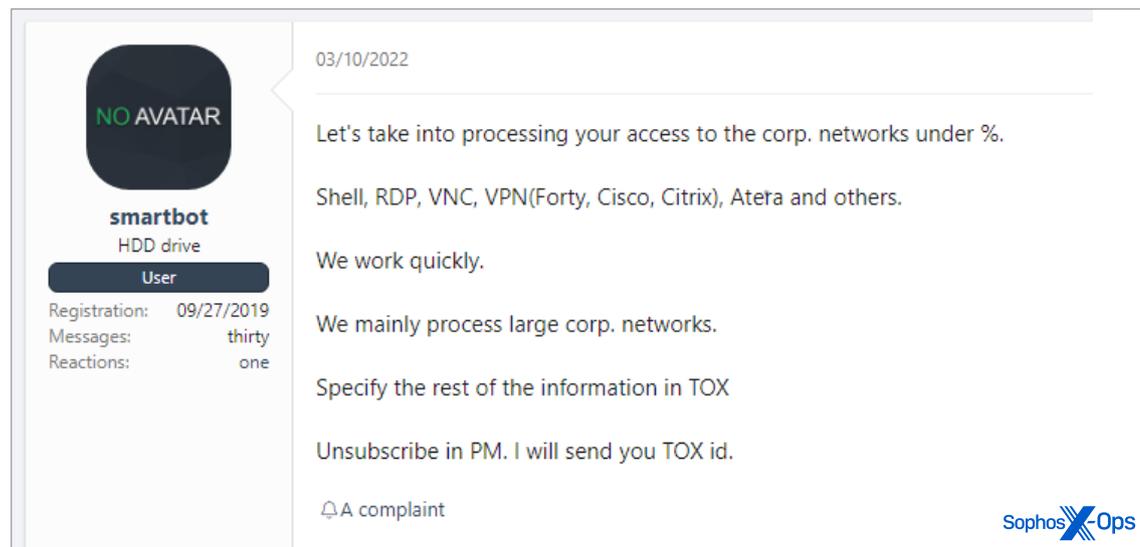


Fig. 33. Offering access to compromised networks via compromised tools

Atera was detected as part of several attempted incursions Sophos investigated, including a series of attempted malware deployments leveraging the Log4J vulnerability and in several ransomware cases investigated by Sophos Rapid Response. In the Log4J exploit attempts, which focused on VMware Horizon servers, the attackers tried to execute a remote PowerShell script to download and install Atera's agent silently with a trial license (along with another abused legitimate remote access tool, Splashtop Streamer). In the Rapid Response incidents, Atera installations were accomplished through exploitation of vulnerable Microsoft Exchange servers. And BlackCat ransomware actors have abused TeamViewer and AnyDesk in recent incidents investigated by Rapid Response.

In many cases, abuse of these legitimate tools can be detected and blocked based on anomalous context, such as strange installation events (for instance, a version of NetSupport being installed by PowerShell into an abnormal directory). Additionally, abuse of these tools can be detected in some cases by the use of a trial license for deployment. Sophos has deployed behavioral rules that detect abuse of Atera's trial license, and continues to develop behavior detection for abuse of this and other remote access packages.

## LOLBins and legitimate executables

A major feature of active adversary attacks, as well as of some more fully automated attacks, is the use of "living off the land binaries," or LOLBins. These native Windows components are leveraged by attackers to execute system commands, bypass preset security features, download and execute remote malicious files, and move laterally across networks.

The leading LOLBin, the Windows command shell (cmd.exe), is used by most backdoors and shells to execute system commands and launch malware, so it is present in practically every malware attack in some form. Each of the Windows scripting platforms – PowerShell, the Microsoft HTML Application Host (mshta.exe), and the Windows Scripting Host (wscript.exe) – are used as tools to execute Windows API calls, download and execute other malicious content, execute system commands and collect data. In addition, PowerShell is used by many of the attack tools used by cybercriminals.

Another frequently abused component of Windows, rundll32.exe, is frequently commandeered by ransomware actors to load malware dropped in dynamic-link library (DLL) format. But there are other legitimate, signed executables that can be similarly abused and are brought along for the task of executing a backdoor or ransomware.

Other LOLBins are not as obvious. The Windows certificate utility (certutil.exe), which can retrieve content from remote web servers, is frequently abused by ransomware operators and other cybercriminals to download and decode malicious files. Bitsadmin.exe, the command-line utility for the Background Intelligent Transfer Service, is used to move files to, from, and within a targeted network without requiring the process that started the transfer to stay live – making it ideal for lateral movement of malware or exfiltration of data.

This type of behavior can be detected and blocked in a number of ways. Malicious behavior using PowerShell and other scripting engines can be detected through monitoring of Microsoft’s Anti-Malware Software Interface (AMSI). Behavioral analysis of the execution of LOLBins through system calls or from a command line can also detect this abuse.

Top ten LOLBins by percentage of computers affected		
LOLBin	Percentage of raw detections	Notes
cmd	92.26%	Default command interpreter
powershell	1.79%	More advanced command-line and scripting shell
certutil	1.09%	Command-line program installed as part of Certificate Services
mshta	1.01%	Microsoft HTML Application Host, allows execution of .HTA (HTML Application)
bitsadmit	0.95%	Background Intelligent Transfer Service, used as part of Windows Update to transfer files
wscript	0.93%	Windows Scripting Host supporting JScript and VBScript execution
bcdedit	0.83%	Command-line tool for managing Boot Configuration Data
rundll32	0.52%	Used to load and run 32-bit dynamic-link libraries (DLLs)
nltest	0.39%	Tool that provides diagnostic information
procdump	0.21%	Command-line application that provides information on system processes

Fig. 34. The ubiquitous cmd.exe is by far the most common target for general LOLBin abuse on Windows systems (April-September 2022).



## “Bring your own” vulnerabilities

Aside from LOLBins, other legitimate executables are often used as part of ransomware attacks and other cybercrime; in this case, the abused apps are brought along by the attacker. In some cases, these are vulnerable executables that can be used to side-load malicious code. This was the case with an archaic McAfee-signed component used in an AtomSilo ransomware attack [last year](#) to deploy a Cobalt Strike backdoor.

Another version of this method is the “Bring Your Own Vulnerable Driver” technique, which leverages a legitimate, signed driver with an exploitable vulnerability to get low-level access to the operating system. For instance, Sophos researchers [found](#) that actors deploying BlackByte ransomware abused RTCore64.sys and RTCore32.sys, drivers used by the widely-used Micro-Star MSI AfterBurner 4.6.2.15658 graphics card overclocking utility. A vulnerability in these drivers (CVE-2019-16098) allows an authenticated user to read and write to arbitrary memory, which in this case was used to bypass and disable some security software.

Other recent incidents deploying the Bring Your Own Vulnerable Driver technique include an unknown attacker abusing a vulnerable anti-cheat driver for the game Genshin Impact in July, and a May report of an AvosLocker ransomware variant abusing a vulnerable anti-rootkit driver from Avast. In both cases, the [drivers were exploited](#) to bypass or shut down security software.

All-up, our Rapid Response team observed activity sufficient to derive a number of useful warning signs that a ransomware attack may be on the way. In a survey of response incidents handled in the first nine months of 2022, at least 83 percent of ransomware were preceded by some indication of trouble. The five most common harbingers of ransomware attack, with their MITRE ATT&CK classifications, were:

- **T1003** – Credential Access – OS Credential Dumping
  - Dumping credentials, either in cleartext or hashed, to gain account login and credential information from the targeted operating system and software
- **T1562** – Defense Evasion – Impair Defenses
  - Modifying or disabling components of the victim’s environment in order to evade or slow down defense measures already in place, including both preventative measures and auditing / logging capabilities
- **T1055** – Privilege Escalation – Process Injection
  - Injecting code into the address space of trusted processes, allowing attacker code to evade defenses and / or elevate privileges; DLL preloading and sideloading fall into this category
- **T1021** – Lateral Movement – Remote Services
  - Using remote services via valid / unprotected accounts to log into a system and perform actions as the logged-on user, perhaps using a RAT or dual-use RAT as described above
- **T1059** – Execution – Common and Scripting Interpreter
  - Abusing command and script interpreters to execute commands, scripts, of binaries, or doing so via interactive terminals or shells, or via remote services as above

A few other patterns spotted were, if not so neatly categorized, of interest to practitioners:

- 64 percent of ransomware attacks (specifically, the deployment of the ransomware) began between 10pm and 6am local time
- The most common time period for the start of attacks was the Monday night / Tuesday morning “overnight shift”
- Exfiltration preceded the ransomware demand phase by approximately two days
- The median attacker dwell time was 11 days

## Ransomware targeting endpoint-security upgrades

In the bullet list above of ransomware attack harbingers, “T1562 – Defense Evasion - Impair Defenses” is worth unpacking further. One development that became more predominant in 2022’s Rapid Response engagements speaks both to Sophos’ success at blocking ransomware from causing damage, and to the recognition of that success by the dominant ransomware groups and their affiliates: Ransomware attacks now routinely involve, as a precursor to deployment of the encryption malware, attempts to access administrative controls that manage the security posture of the target.

As described in an earlier section, ransomware’s “active adversaries,” the people who engage in hands-on-keyboard activities during an attack, routinely use password-sniffing or scraping tools in order to capture administrative credentials. Threat actors abuse utilities like Mimikatz, originally created as a tool for improving security, to sniff and extract user passwords from the networks of attack targets.

Previously, these administrative passwords were then used to take control of management tools (such as Windows Domain Controllers) that the attackers could leverage to deploy the ransomware itself. But in more recent attacks, attackers are increasingly using these credentials to access the central controls used to manage endpoint security protection. In some cases, attackers immediately used those stolen credentials to log into those central management tools and disable tamper-protection features in those endpoint security tools, or in some cases to disable endpoint security altogether.

To thwart these types of attacks, Sophos and other companies have added multifactor authentication (MFA) features into the central management console login pages, as well as into physical devices like firewalls, which have administrative logins. But the end users of these products - the security and IT administrators - still need to enable those features and register to use them before they can be effective at stopping threat actors. Sophos encourages all its customers to enable those protections as soon as feasible.

## Miner malware

Cryptocurrency mining software consumes computing power to perform cryptographic work in hopes of earning new “coins” (tokens), usually participating as part of a networked pool of processors or machines. For many cryptocurrencies, mining requires specialized hardware with graphics processing units dedicated to the processing-hungry work. But there are still opportunities for exploitation of general-purpose hardware to mine cryptocurrency—and there are vast self-spreading networks of mining bots that still attempt to exploit vulnerable systems and steal processing power for profit.

While such malware does not impact organizations’ data, it does sap computing resources, and raises electrical and cooling costs. And miner malware is often the harbinger of other malware, as it is usually deployed via easily exploitable network and software vulnerabilities.

Most miner malware is focused on Monero (XMR), for a number of reasons. The type of work required to produce XMR doesn’t necessarily require specialized graphics cards, which means that it can be mined with servers that don’t have much in the way of graphics hardware. And XMR is less traceable than many other cryptocurrencies, making it more attractive for criminal activity.

Miner bots are often the first malware to exploit newly published vulnerabilities. The Log4J Java vulnerability and the ProxyLogon/ProxyShell exploits of Microsoft Exchange Server were quickly leveraged by miner botnets. In many Rapid Response ransomware cases, Sophos responders found evidence of miner malware using the same point of initial compromise as the ransomware – in some cases months before the ransomware attack.

Miners are also a cross-platform problem. While many of the miner malware bots Sophos detects are Windows-based (and leverage PowerShell and other Windows scripting engines to install and persist), there are Linux versions of these botnets as well — often targeting unpatched network appliances or web servers.

While XMR miners are still prevalent and popular, fluctuations (mostly in the negative direction) of the value of some cryptocurrencies have had an effect on miner operators. As XMR's value has dropped, the profitability of miner botnets has declined, and it appears to have had an impact on how much effort bot operators make to grow their mining pools. Some fluctuations in detection rates for miner deployments have followed the fluctuations in XMR's value, as shown below. Note in particular the drop in mid-June of both XMR value and miner detections.

#### Monero miner detections and price fluctuations, April-September 2022

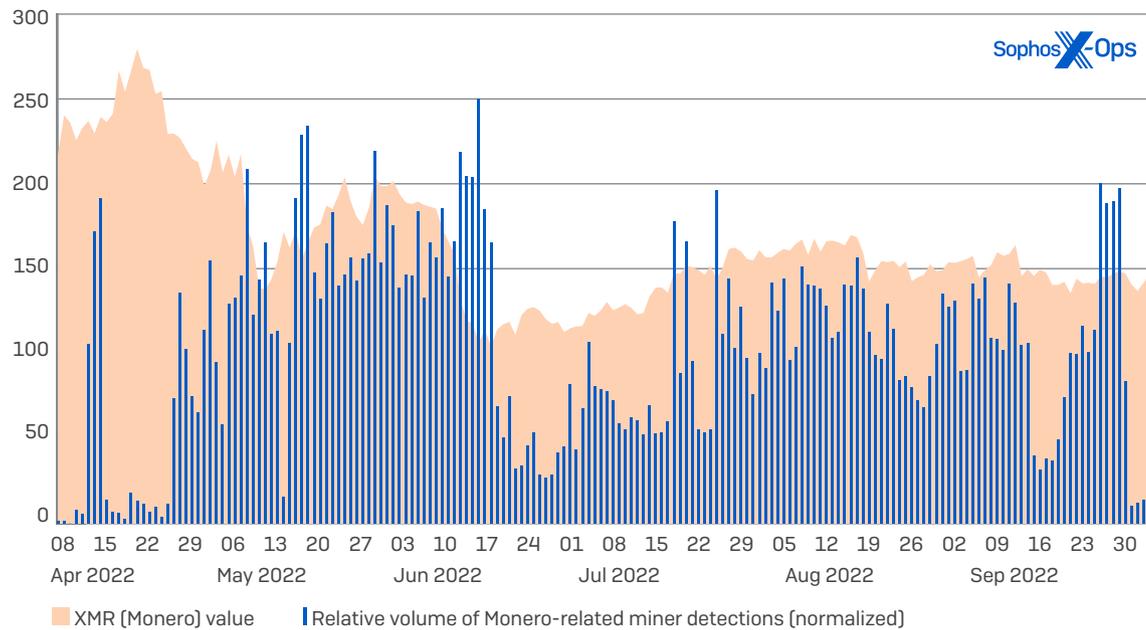


Fig.35. Monero detections over the past year (in blue, totals normalized for scale) show some congruence with Monero values during the period (in orange).

But the profitability of miners is affected by not only the value of the currency being mined, but the longevity of the miner; many miners actually hunt for and remove similar miners from servers that they exploit. In some cases, miners even deploy patches to fix the vulnerabilities they used to install to prevent other miners from uprooting them—allowing them to persist when organizations do scans for vulnerable systems.

## Beyond Windows: Linux, Mac, and mobile threat landscapes

To this point in our report we've spoken primarily of malware and attack tooling affecting Windows; that's expectable, considering Windows' pre-eminent place in the targeting lists of most attackers. However, Windows is not the only viable target in the enterprise, and we increasingly hear about attack campaigns with payloads that "support" multiple platforms. These are built either by using multiplatform-supporting languages such as Go or Python (often wrapped in pyinstaller) or frameworks like Electron, or by preparing binaries for all major frameworks. In this final section, we'll briefly look at the Linux, Mac, and mobile-platform threat landscapes, with the caveat that many of the miners in particular are – again – present across all these platforms and others.

### Linux threats

Linux systems have long been a target for the services that are most frequently deployed on that operating system, including organizational websites, virtual-machine servers, network appliances, storage servers, and enterprise application infrastructure. Increasingly, criminals are developing cross-platform ransomware and other malware to allow them to better target those resources for profit. In the first six months since Sophos unveiled its Linux protections, we detected 14 individual Linux servers targeted by ransomware.

Much of the malware affecting Linux systems (as well as other server platforms) is built to mine cryptocurrency. Over 40 percent of all our detections, and 72 percent of individual Linux devices detected with malware, are the result of miners.

Linux threats by percentage of Linux detections		
Threat	Percentage of detections	Notes
Miner	43.0%	Generic miner detection
DDoS	27.1%	Mirai-related detection
Tsunami	12.3%	IRC-based DDoS client
Gognt	11.5%	Generic detection for malware written in Go
Rst	1.3%	Twenty-year-old file-infector virus
Loit	1.1%	Local exploit
Swrort	0.9%	Mettle (Meterpreter implementation) for Linux
SSHDoor	0.7%	SSH backdoor
XpMmap	0.6%	Memory-related exploits
DrtyCoW	0.6%	Dirty COW (CVE-2016-5195) exploit
ProcHid	0.4%	Process-hiding Trojan
Ngioweb	0.2%	Proxy botnet
Psdon	0.1%	Poseidon agent for Mythic red teaming framework
GoScan	0.1%	Go scanner looking for vulnerable machines

Fig. 36. Despite chaos on the cryptocurrency scene in 2022, miners are an unfortunately reliable infection type on Linux.

Miners have dominated the Linux findings this year – even more thoroughly than this chart suggests. “Miner” is the generic Sophos detection for a miner. Miners can also be detected under other names; for instance, “Gognt” is our detection for otherwise unrelated malware families written in Go. This means that there are likely miners outside of the “miner” detection, meaning there are even more than shown here.

Linux threats by percentage of unique Linux detections		
Threat	Percentage of unique machines	Notes
Miner	74.3%	Generic miner detection
Gognt	5.1%	Generic detection for malware families written in Go
DDoS	4.3%	Mirai-related detection
Swrort	3.2%	Mettle (Meterpreter implementation) for Linux
DrtyCoW	3.1%	Dirty COW (CVE-2016-5195) exploit
Ngioweb	2.8%	Proxy botnet
Tsunami	2.7%	IRC-based DDoS client
Roopre	0.9%	Backdoor targeting Web servers
SSHBrut	0.9%	SSH brute force password cracker
Loit	0.8%	Local exploit
Shell	0.8%	Malware giving shell access to the attacker
Bckdr	0.6%	Generic backdoor detection
Ransm	0.6%	Ransomware

Fig. 37. When broken out by unique machines affected, the impact of miners in the Linux space is even clearer.



The next largest groups of Linux detections on affected systems are associated with Gognt and with distributed denial of service (DDoS) toolkits. Nearly all of these malware target vulnerabilities have been addressed in more recent versions of Linux, but remain unpatched on a sizeable number of devices and appliances.

There are several backdoors and botnets among the remaining major Linux threats, but perhaps the most interesting of the other top threats to the platform from an enterprise perspective is Tsunami, a long-running Linux backdoor that has recently evolved to target Jenkins and WebLogic application servers.

## Mac threats

In 2022, we noted increasing numbers of open-source attack tools and post exploit/C2 frameworks that support macOS could be found on places like GitHub. The mere presence of code on the repository doesn't exactly correlate to some surprise explosion of big Mac attacks, but it does likely indicate at least an increase in interest – and a willingness to share.

On the macOS platform, the primary threat continues to be potentially unwanted applications, including apps that install plug-ins for Apple's Safari browser (as well as other browser platforms). These apps inject content into web pages in order to redirect users to fraudulent or malicious content.

Potentially Unwanted Applications (PUAs) on macOS, April-September 2022		
Detection	Percentage of unique machines	Notes
Adloadr	16.2%	Generic adware detection
Genieo	8.9%	Browser [search] hijacking
Bundlore	8.4%	Adware
Dynji	4.6%	Browser [toolbar] hijacking
Pirrit	3.7%	Adware
AdvMac	3.2%	Adware
HistColl	3.0%	Browser data collection
Keygen	2.3%	Software piracy tool

Fig. 38. Adloadr leads the list of Mac PUAs in 2022 by a healthy margin.



The Adloadr application, one of several prevalent PUAs characterizable as adware, shot up to the top place in our Mac telemetry statistics in 2022 with nearly twice as many infections of unique machines as the browser-hijacking Genieo, in second place.

On the malware side of things, we observed high counts of NukeSped, VSearch, and Dwnldr – a remote-access Trojan, an adware package, and a general-purpose downloader Trojan detection. Chropex and ProxAgnt, two helper apps associated with the Adloadr family, also appeared in our list of common detections.

Malware detections on macOS, April-September 2022		
Detection	Percentage of unique machines	Notes
NukeSped	22.2%	Remote-access Trojan
VSearch	15.6%	Adware / browser hijacking
Dwnldr	10.8%	Generic Trojan detection
Agent	10.8%	Generic malware detection
Keygen	6.4%	Key generator to circumvent copy protection
FkCodec	6.2%	Adware; pretends to be video codec installer
Chropex	5.0%	Adware; also exhibits browser hijacking behavior
ProxAgnt	1.9%	Trojan
Swrort	1.5%	Remote-access Trojan

Fig. 39. NukeSped, VSearch, and Dwnldr top the macOS malware-detections leaderboard.



We've spotted five new-for-2022 macOS threats of note as of October; none of the five made the top of our macOS malware charts, but we're observing them with interest and fresh detections.

Newly observed macOS threats for 2022			
Month	Name	Detection	Notes
January	SysJoker	OSX/SysJoker	Multiplatform backdoor that supports macOS
January	DazzleSpy	OSX/DazzleSpy	Infection technique related to MACMA, a backdoor that targeted Hong Kong democracy activists
March	Gimmick	OSX/Gimmick	Communicates via Google Drive APIs to hide network traffic from monitoring systems
May	pymafka/CrateDepression	Troj/Pymaf, OSX/Cobalt	Supply chain attack on package hosted on pypi; eventually drops Cobalt Strike beacon
October	Alchemist	Exp/20214034-D	Multiplatform attack framework written in Go

Fig. 40. Five novel macOS threats emerged in the first ten months of 2022.



## Mobile threats

Because mobile applications have become the dominant way in which people interact with the internet, mobile devices are at the center of a burgeoning range of new types of cybercrime. While the Android platform still sees a steady flow of malware delivered in the form of fake applications and information stealers, both Android and iOS have increasingly been targeted by fraudulent and fake applications—and criminals have found ways to use social engineering to breach even the walled garden of Apple's mobile devices.

Malware injectors, spyware and banking-associated malware still lead the field in terms of malicious Android .APK packages in our detection, along with apps that generate fake ad clicks. But potentially unwanted applications—including apps that essentially do nothing but act as a way of collecting hidden “in-app purchases” from victims—continue to grow as a threat to mobile users. And the last year has seen the emergence of a sophisticated set of financial fraud rings, using fake apps, that has become an industry in Southeast Asia.

Sophos began tracking an organized crime campaign we dubbed CryptoRom in 2021. The campaign is based on a form of cyberfraud, known as sha zhu pan (杀猪盘) – literally “pig butchering plate” – and is backed by a well-organized syndicate of fraudulent web and application developers, fake social profile builders, and individuals who engaged in scripted social engineering efforts via social media and dating apps to ensnare victims in the scam.

In October of 2021, we documented the campaign's [global expansion](#). The formula has shifted and mutated, swinging from fake cryptocurrency investment to fake crypto derivative investments, and into other fake financial markets. To make these schemes seem legitimate, the rings create fake applications and mobile websites that impersonate legitimate financial institutions. Many of these apps have slid undetected into app stores, such as “liquidity mining” apps that were found in the Apple App Store and Google Play store.

Meanwhile, the scammers have found ways to abuse iOS as well, leveraging Web Clips and application developer test deployment programs to get their applications onto iOS devices. This includes the abuse of Apple's “Super Signature” ad-hoc distribution scheme, “Test Flight” beta testing, and enterprise application schemes to avoid Apple's App Store security screening. The same approach may be used for other iOS-targeted malware, but requires some social engineering of the target to allow the installation to go forward.

These applications have resulted in hundreds of millions of dollars in losses to victims, and are part of an ever-growing ecosystem of cybercrime that has spread from romance-driven engagement to broad social engineering attempts on platforms such as Facebook, Twitter, and LinkedIn. The scams continue to evolve and are being copied by other crime rings, each with their own particular twist.

Both Android and iOS are also targets for malicious advertising campaigns, including fake alerts that mimic system alerts—often directing users to an app store to purchase an application that has hidden subscription fees, installs other malware, or both.

Sophos continues to work on ways of blocking these threats, and alerts mobile OS developers to new abuses of their app stores as they are discovered.

## Conclusion

Across the entire threat landscape, two things stand out: the continuous lowering of barriers to entry for would-be cybercriminals and the commodification of what once would have been considered “advanced persistent threat” tools and tactics. While there has long been a thriving marketplace for hacking tools, malware and access to vulnerable networks, the lessons learned from the recent history of ransomware operations and other well-funded malicious actors are more rapidly becoming available to the wider criminal community—as are commercial security tools designed to defeat some defenses.

Geopolitical conditions have continued to make fighting cybercrime more difficult. This year, China ended cooperation with US law enforcement in fighting cybercrime as US-China relations became more tense; meanwhile, as China increased its crackdown on domestic cryptocurrency scams and other cybercrime, Chinese-language criminals rapidly shifted toward export of these criminal operations. And while the war in Ukraine briefly disrupted some Russian-language crime rings, they quickly reconstituted.

There is no sure defense against all these threats. Active defense is required to prevent incursions from doing damage, and the burden of defense is too great for many organizations to shoulder themselves. Sophos continues to work to increase its capabilities to aid organizations of all sizes against the continually evolving threat landscape through endpoint and network defenses and managed security operations services.

United Kingdom and Worldwide Sales  
Tel: +44 (0)8447 671131  
Email: [sales@sophos.com](mailto:sales@sophos.com)

North American Sales  
Toll Free: 1-866-866-2802  
Email: [nasales@sophos.com](mailto:nasales@sophos.com)

Australia and New Zealand Sales  
Tel: +61 2 9409 9100  
Email: [sales@sophos.com.au](mailto:sales@sophos.com.au)

Asia Sales  
Tel: +65 62244168  
Email: [salesasia@sophos.com](mailto:salesasia@sophos.com)