proofpoint.

REPORT

2022 Spring/Summer Threat Summary

State-sponsored attacks, major-league malware and phishing for cryptocurrency

proofpoint.com

Cyber Crime Under the Spotlight

Welcome to the Spring/Summer Threat Summary. This installment recaps campaigns from the first half of 2022.

At the start of the year, conflict between Russia and Ukraine threatened the world's first full-scale cyber conflict. As it turned out, those predictions proved wide of the mark. But the ongoing humanitarian crisis has still had a significant impact on the cybersecurity landscape. Most obviously, several state-sponsored actors took advantage to launch attacks. But as we'll see, the conflict had other consequences, including revealing the inner workings of one of the world's most successful ransomware groups. The ongoing humanitarian crisis has still had a significant impact on the cybersecurity landscape.

Beyond issues arising from the Russia-Ukraine conflict, Microsoft's decision to block macros for downloaded documents set off a chain reaction of ingenuity in attack techniques. And new malware continues to appear on the landscape. Finally, surging consumer interest in cryptocurrency has delivered a new set of targets for phishing and financially motivated cyber crime. As usual, while this report will explore many new techniques, our focus remains the human factors that allow cyber criminals to undermine security and breach defenses.

State-Aligned Activity

As we shared in this year's Human Factor report, **advanced persistent threat** (APT) activity is rarer than financial cyber crime. But with governments, media organizations and humanitarian efforts among those targeted, the stakes are high.

At the start of the year, tension between Russia and Ukraine erupted into open warfare. For certain state-sponsored groups, the violence and upheaval presented an opportunity.

advanced persistent threat

APT actors are state-sponsored or state-aligned adversaries, typically involved in espionage or sabotage rather than financially motivated cyber crime.

Profiting from upheaval

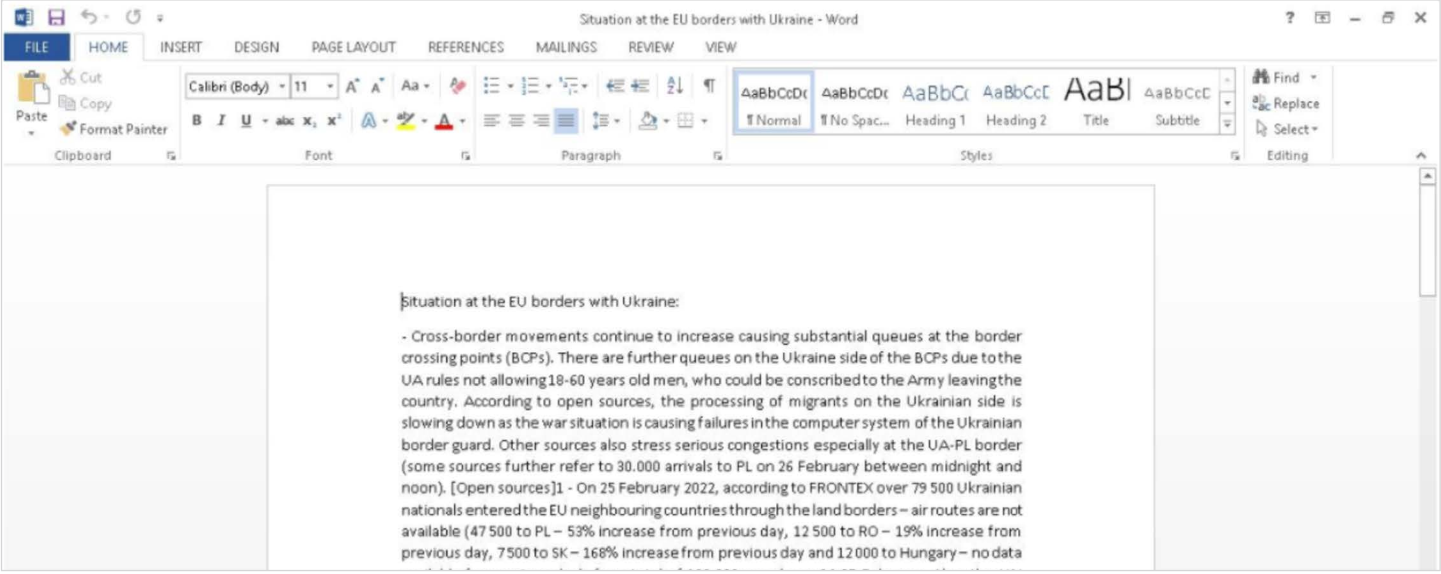
In early March, our researchers published details of a likely APT phishing campaign targeting European government entities responding to the refugee crisis. Dubbed "Asylum Ambuscade," the campaign used a compromised email address belonging to a member of the Ukrainian armed forces. Message lures mentioned NATO and contained an attachment that attempted to download a novel malware dubbed "SunSeed." The purpose of the attacks may have been intelligence gathering.

The web bugs bite

Shortly after the emergence of Asylum Ambuscade, we reported on activity from **TA416**. This China-aligned group also targeted European diplomatic entities, including those involved in refugee and migrant services. Since 2020, TA416 has maintained a consistent set of TTPs. The group is known for using "web bugs" (also called "tracking pixels") to profile potential victims. Web bugs are embedded in email as non-visible objects. When the email is opened, the object is downloaded from the attacker's server, confirming that an address is active.

TA416

This actor is believed to be associated with Chinese state interests. Historically the group has targeted dissident factions in Southeast Asia, but more recently it has been observed pursuing targets in Europe.



Situation at the EU borders with Ukraine:

- Cross-border movements continue to increase causing substantial queues at the border crossing points (BCPs). There are further queues on the Ukraine side of the BCPs due to the UA rules not allowing 18-60 years old men, who could be conscribed to the Army leaving the country. According to open sources, the processing of migrants on the Ukrainian side is slowing down as the war situation is causing failures in the computer system of the Ukrainian border guard. Other sources also stress serious congestions especially at the UA-PL border (some sources further refer to 30.000 arrivals to PL on 26 February between midnight and noon). [Open sources]1 - On 25 February 2022, according to FRONTEX over 79 500 Ukrainian nationals entered the EU neighbouring countries through the land borders – air routes are not available (47 500 to PL – 53% increase from previous day, 12 500 to RO – 19% increase from previous day, 7500 to SK – 168% increase from previous day and 12 000 to Hungary – no data

Figure 1. A decoy Word document used by TA416.

PlugX

A remote access Trojan of Chinese origins, typically used as a first stage malware to gain a foothold in target networks.

TA412

An APT actor believed to operate from China. Reporting from Microsoft identifies the group by the name "Zirconium" and has identified them as responsible for activity during the 2020 U.S. elections.

TA459

An APT actor operating from China. Primarily employs spear phishing with exploit-laden Microsoft Word documents and RAR archives.

Chinoxy

A backdoor malware typically seen in campaigns targeting entities in Southeast Asia.

Using web bugs may allow TA416 to be more selective in sending out malware. With fewer copies circulating, there's less chance of malicious code falling into the wrong hands. For the past two years the group has used **PlugX** malware. Analysis over that period suggests that TA416 has been steadily improving PlugX to stay ahead of defenders.

Media matters

In July we published a review of APT attacks against news media. Among the reported campaigns was activity by two other Chinese groups who targeted outlets reporting on the Russia-Ukraine conflict.

In February 2022, **TA412** launched a series of attacks against U.S.-based media. The group sent messages with subject lines about U.S. and European government intervention in the conflict. The emails contained web bugs that gathered IP addresses and User-Agent strings. TA412 may collect this information as a prelude to more targeted phishing activity.

In April, another Chinese APT group known as **TA459** targeted journalists reporting on the conflict with malicious RTF files. If opened, the RTF file installed **Chinoxy**, which sets up a persistent backdoor on the victim's machine.

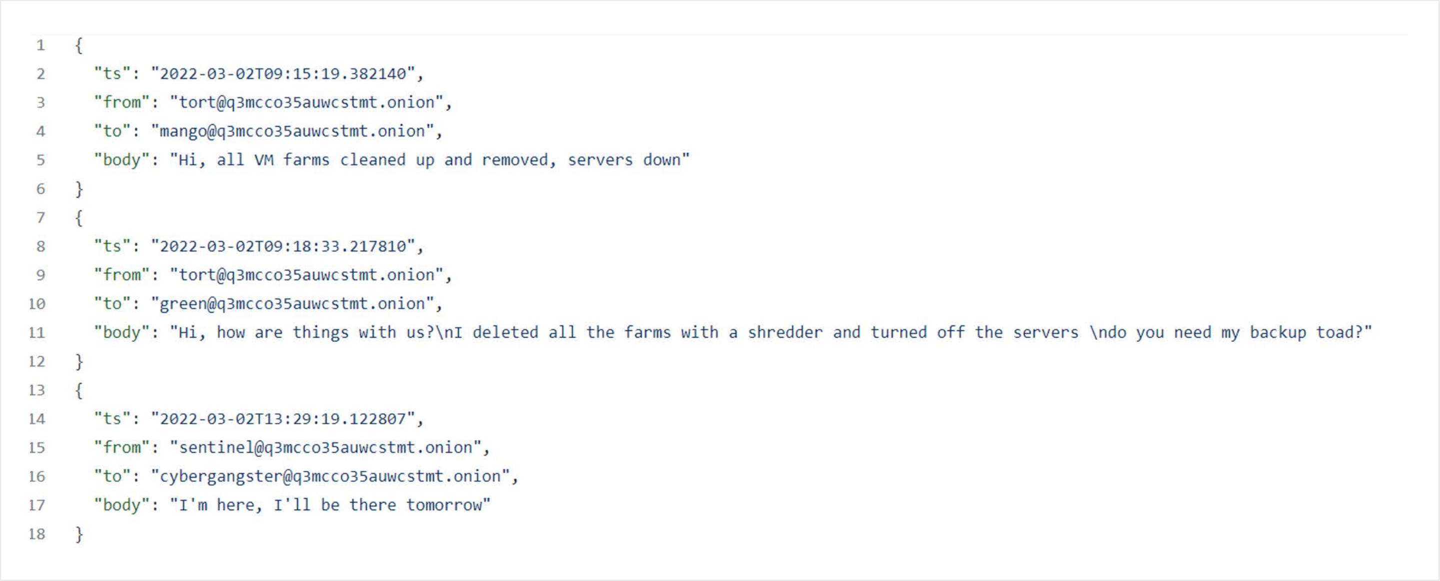
Major League Crimeware

Conti

One of the world's most successful, and by some accounts ruthless, ransomware operators. It came to prominence in early 2021 with attacks on healthcare services in the U.S. and Ireland, a sector traditionally considered off-limits.

In March, a Twitter account called @ContiLeaks released chat logs and files belonging to **Conti**, arguably the world's most successful ransomware group.

The leaks began after Conti made a public statement siding with Russia—apparently angering those who opposed the country's invasion. The logs contained everything from insights into Conti's organizational structure to its negotiating tactics and relationships with high-profile malware families.



```
{
  "ts": "2022-03-02T09:15:19.382140",
  "from": "tort@q3mcco35auwcstmt.onion",
  "to": "mango@q3mcco35auwcstmt.onion",
  "body": "Hi, all VM farms cleaned up and removed, servers down"
}
{
  "ts": "2022-03-02T09:18:33.217810",
  "from": "tort@q3mcco35auwcstmt.onion",
  "to": "green@q3mcco35auwcstmt.onion",
  "body": "Hi, how are things with us?\nI deleted all the farms with a shredder and turned off the servers \ndo you need my backup toad?"
}
{
  "ts": "2022-03-02T13:29:19.122807",
  "from": "sentinel@q3mcco35auwcstmt.onion",
  "to": "cybergangster@q3mcco35auwcstmt.onion",
  "body": "I'm here, I'll be there tomorrow"
}
```

Figure 2. Jabber logs leaked by @ContiLeaks Twitter handle.

Conti shut down the leaks, but announced a new business model in May. Its members would partner with other operators, providing access and expertise but keeping a lower profile. It's easy to imagine that this drastic change was prompted in part by scrutiny arising from the leaks.

Emotet gears up

The disappearance of Conti as a direct ransomware threat might seem like good news. But the group's close ties to Emotet mean it isn't time to celebrate yet. After reemerging late last year, Emotet activity has returned to familiar volume highs mixed with a handful of experimental techniques.

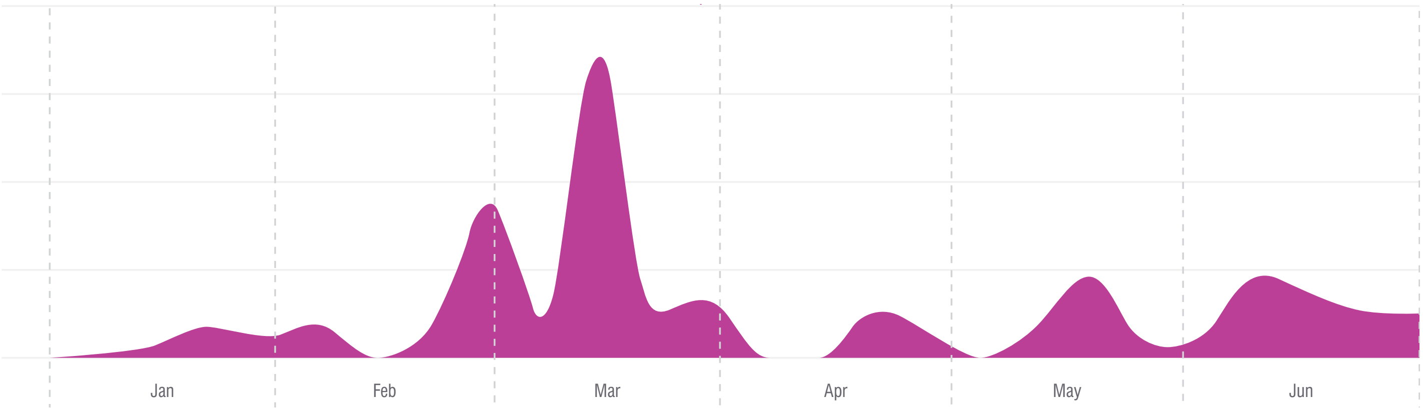


Figure 3. Emotet weekly message volume, H1 2022.

Emotet/TA542

Before the 2021 takedown of its infrastructure, Emotet was the world's most frequently distributed malware. Since returning at the end of the year, Emotet's distributor, known as TA542, has been linked with the Conti group.

Like many high-volume threat actors, **Emotet/TA542** often takes seasonal breaks. During a "spring break" pause in regular activity, we observed a low-volume campaign using new delivery methods. Most of Emotet's high volume activity uses attachments or links to infected Office files. But in these experimental campaigns, emails included OneDrive URLs leading to XLL files. Experimenting with techniques beyond macro-enabled documents—historically a leading attack technique—may be a response to Microsoft's decision to disable macros by default for Office users.

It's worth noting that Emotet activity coincided with the Russian invasion. Some members had expressed support of the invasion, which created internal friction that led to the group's breakup.

Bye Baza, hello Bumblebee

The trove of leaked Conti documents also highlighted the group's involvement with BazaLoader. This malware was a regular sight throughout 2021, but as of February this year it disappeared from our data. Its successor, known as Bumblebee, uses some elaborate techniques to remain hidden, including being able to detect when it is running (and being observed by security tools) on a virtual machine.

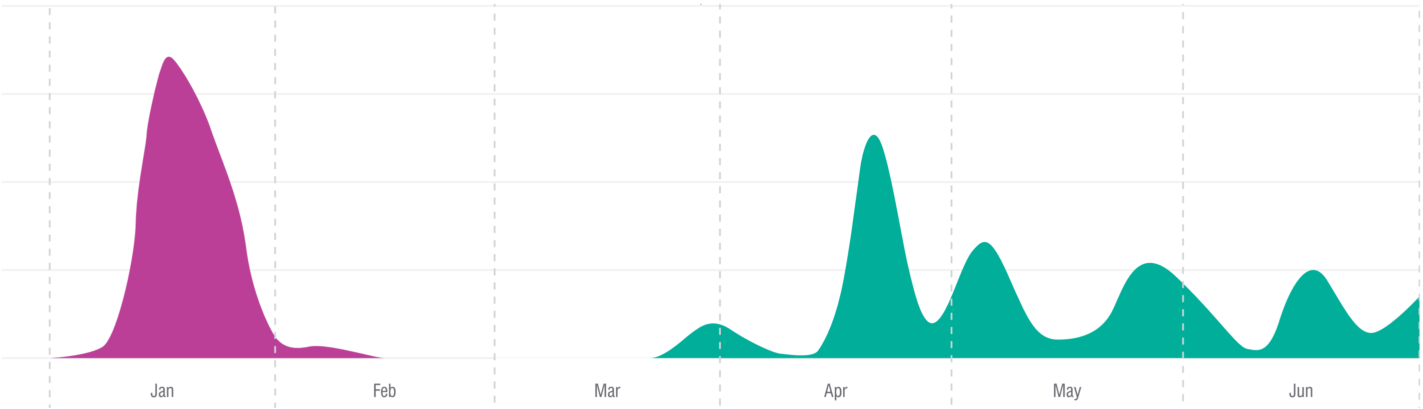


Figure 4. BazaLoader and Bumblebee message volume, H1 2022.

Since first appearing in March, we've seen evidence that Bumblebee is being actively developed, gaining new functions, including encrypted communications and enhanced defense against analysis. It's possible that information about BazaLoader in the Conti leaks prompted the switch to a new loader.

New Malware on the Block

Emotet and other evergreen malware dominated the threat landscape in sheer volume. But there's been no lack of innovation among crimeware developers. In the first six months of 2022, our researchers encountered several novel strains of malware.

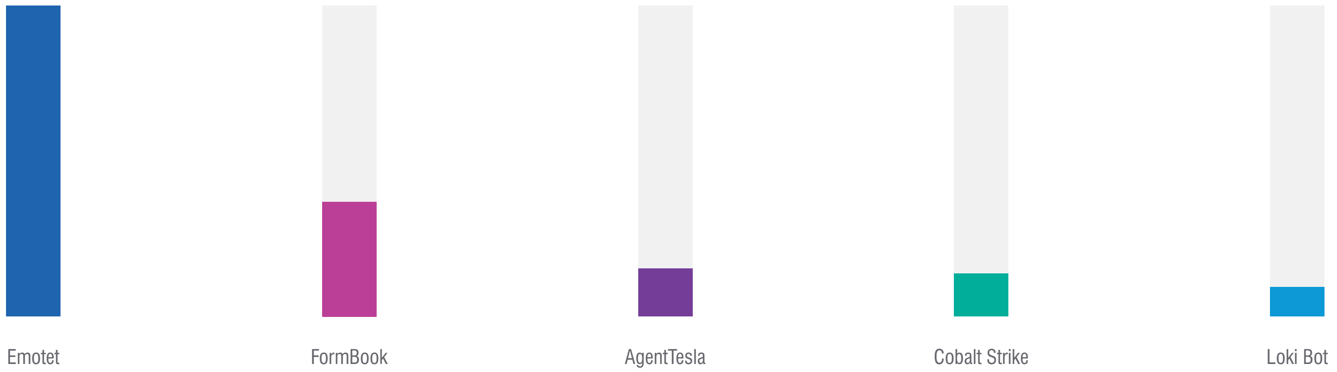


Figure 5. Top malware by message volume H1 2022.

Nerbian Rat

This Trojan is notable for its anti-analysis and anti-reverse-engineering capabilities. As we explored in last year's Fall/Winter Threat Report, malware developers are turning to obscure programming languages to evade detection. Nerbian Rat is written in GO and makes use of several open-source libraries to automate its activities.

In common with many other strains, this malware was distributed as a malicious Office document. Campaigns used COVID-19 lures. Infection occurs in two stages. First, an initial dropper payload performs reconnaissance to ensure that it has been downloaded on a genuine target system. Once this is established, the secondary RAT payload is downloaded. As for the name? A function in the malware seems to be named after Nerbia, a fictional duchy in Don Quixote.

Serpent backdoor

In March, our researchers documented a new backdoor malware being distributed using the Chocolatey package installer. They called this malware "Serpent" after a piece of ASCII art embedded in the VBA macro used to distribute the installer. The attack chain contains a rare use of steganography; a PowerShell script installs Chocolatey embedded in an image of Swiper, a character from the cartoon "Dora the Explorer."

Figure 6. "Swiper" image with base64 encoded PowerShell script.

The campaigns distributing Serpent targeted French organizations in construction, real estate and government sectors. Message lures were styled as GDPR updates for job candidates.

DTPacker

Back in December 2020, our researchers wrote about the rise of "packer" software. Packers help malware evade detection by hiding the payload within a benign wrapper file. In January of this year, we saw a new packer distributing multiple strains of **commodity malware**. After discovering reference to a former U.S. president in the packer's code, our researchers named it DTPacker.

DTPacker uses obfuscation to evade antivirus, sandboxing and analysis. In early campaigns it was downloaded from locations related to Liverpool Football Club, though no obvious reason for this affiliation was uncovered.

commodity malware

Malicious applications that can be bought outright or purchased on a SaaS model from developers on criminal forums or the dark web. Generally well-understood and with a long presence in the threat landscape. Examples include Agent Tesla, Ave Maria and FormBook.

OiVaVOi

Finally, in January our researchers also detected a hybrid cloud attack making use of malicious **OAuth** apps. This technique was nicknamed "OiVaVoi" after a domain used in the attacks. Several accounts belonging to C-level executives were compromised because of the activity.

This attack worked by using compromised "verified publisher" accounts to create malicious OAuth applications. Requests were then sent to victims, asking them to authorize the application on their account. Because the requests appeared to come from a legitimate source, many victims agreed. This gave attackers persistent access to the account as well as the ability to generate further OAuth tokens.

OAuth

An open-standard authentication protocol that uses tokens to provide access to online services without requiring passwords. Commonly encountered when using Facebook or Google credentials to access third-party sites and applications, but also found in some enterprise cloud environments.

Social Engineering Developments

A convincing lure is arguably the most powerful asset in a cyber attacker's tool kit.

With the right social engineering, even the least sophisticated malware can still find its way through. In this section we'll cover a few key developments in lures and targeting. But for a more thorough exploration of social engineering, check out the recent report written by our Threat Research group.

Moving away from macros

In February, Microsoft announced that it would begin blocking VBA macros in downloaded Office documents. This followed a decision in October 2021 to do the same for the older XL4 format. Malicious macros have been a favorite malware distribution method for more than two decades, so Microsoft's announcement precipitated immediate shifts in threat actor behavior. Between October 2021 and June 2022, our data shows a 66% decline in malicious use of macro-enabled attachments.

Threat actors immediately began experimenting with alternative distribution vehicles. Several file types have seen substantial growth.

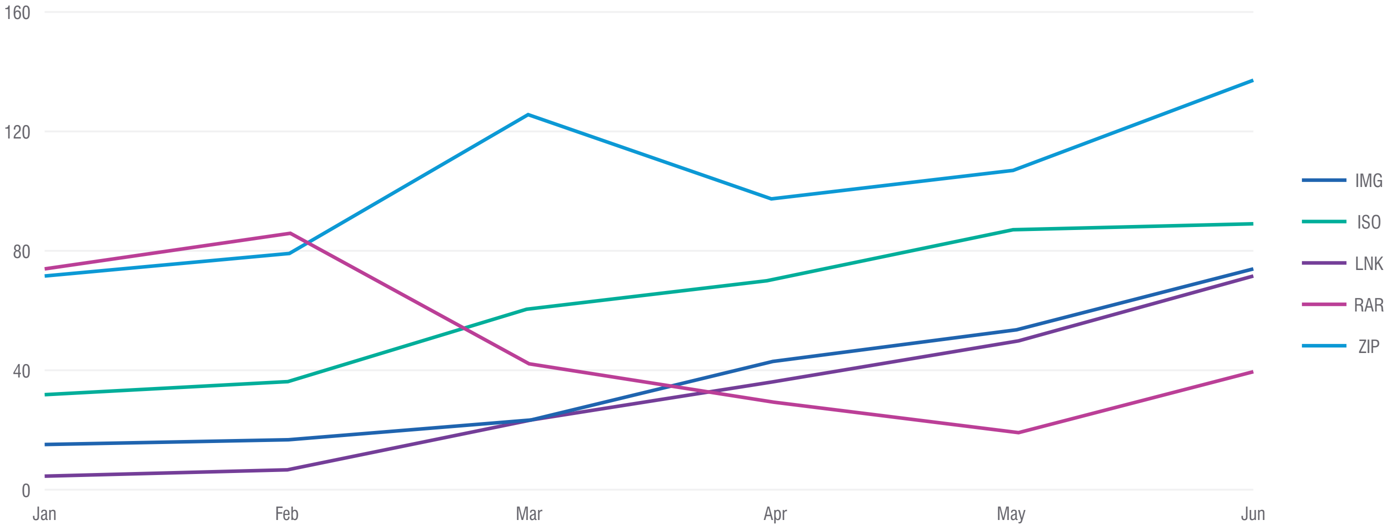


Figure 7. Growth of alternative file types for threat delivery.

Still, the growth of these alternative file types doesn't mean that macros have gone away. The method Microsoft relies on to block macros is based on a Mark of the Web (MOTW) attribute. MOTW is added to files when they are downloaded from the internet. But crucially, it isn't added if the file is downloaded within another container, such as a RAR or ZIP archive or an ISO image. In these cases, the container file receives a MOTW, but the contents do not. Through this interstitial payload, malicious Office documents can still make their way to victims, with all the potential for social engineering that entails.

Beyond macro-enabled files, we've also observed containers being used to deliver malware directly using LNK, DLL or EXE files. Together, these changes represent one of the largest threat landscape shifts in recent years.

Phish kits

We've been tracking developments in the world of commodity phishing software for some time. These toolkits lower barriers to entry and can be purchased for as little as $10. They contain everything you need to set up a phishing page, including templates, logos and other site assets. At the more expensive end of the spectrum, we've also seen kits capable of stealing multifactor authentication (MFA) tokens and session cookies in real time.

Some of the most sophisticated kits currently available use a **transparent reverse proxy** to do away with the need for creating a spoof site altogether. In these attacks, the actual target website is presented, greatly enhancing the victim's trust. The threat actor sits as a "man in the middle," harvesting usernames, passwords, MFA tokens and session cookies; all while the victim seemingly engages with a familiar site as normal. The criminal can then use these credentials to immediately change passwords, copy data and disable alerts.

transparent reverse proxy

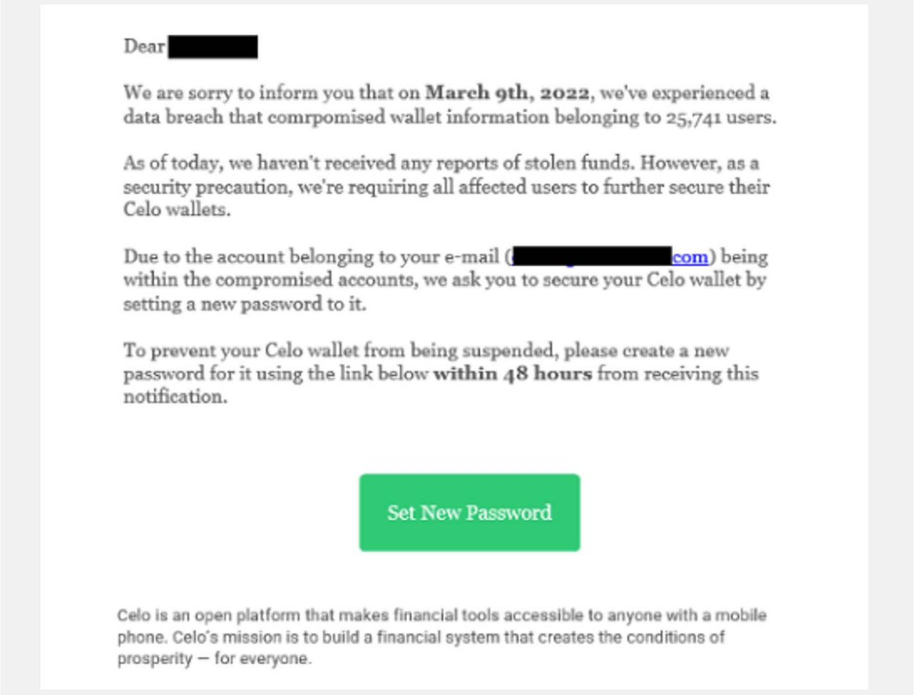
Proxies are servers that sit between an end-user and the internet. A transparent proxy does so without altering traffic. They have legitimate uses, but threat actors utilize them to operate "man-in-the-middle" attacks, harvesting credentials while victims engage with a real website.

But if you're just too time or resource constrained to spin up your own hosting, phishing as a service (PhaaS) is also on the rise. For only a few hundred dollars a month, PhaaS providers offer a turnkey solution, covering templates, email distribution, servers and credential collection. One of the more popular PhaaS services has more than a hundred templates, with sites constantly added and updated.

Crypto woes

Nine-figure hauls from Horizon Bridge and Axie Infinity have already made 2022 a year of record-breaking cryptocurrency thefts. So, it's no surprise that crypto has also been a popular target for email-based phishing and malware.

Many of the features that make Bitcoin appealing also make it risky. There is no government backing your funds. And because digital assets are easily transferred, crypto tokens are as vulnerable to theft as any other piece of data. Accordingly, cryptocurrency and loss-aversion lures go hand in hand. The risk of compromised wallet credentials is real. So security alerts asking users to reset passwords are highly likely to succeed. In fact, the popularity of this threat creates a virtuous cycle for attackers. Each incident of a wallet being emptied with stolen credentials increases user anxiety that they will be next.



Dear [redacted]

We are sorry to inform you that on **March 9th, 2022**, we've experienced a data breach that comrpomised wallet information belonging to 25,741 users.

As of today, we haven't received any reports of stolen funds. However, as a security precaution, we're requiring all affected users to further secure their Celo wallets.

Due to the account belonging to your e-mail ([redacted]com) being within the compromised accounts, we ask you to secure your Celo wallet by setting a new password to it.

To prevent your Celo wallet from being suspended, please create a new password for it using the link below **within 48 hours** from receiving this notification.

Celo is an open platform that makes financial tools accessible to anyone with a mobile phone. Celo's mission is to build a financial system that creates the conditions of prosperity — for everyone.

Figure 8. A bogus crypto wallet password reset alert.

As cryptocurrency is borderless by design, attacks aren't just limited to English speakers. In May 2022, Portuguese speakers in Brazil were targeted with a Binance-themed campaign that tried to steal recovery passphrases. Similarly, German language users were targeted the same month by attackers seeking login credentials for OpenSea, the popular NFT trading platform.

In many of these cases, convincing fake landing pages were created with phish kits. Seeing templates for popular cryptocurrency platforms alongside traditional banking sites is a sure sign of where financially motivated threat actors see their next payday.

Conclusion and Recommendations

As these highlights show, the threat landscape was a dynamic place in the first half of the year.

Defenders had to react to external circumstances even as they tried to keep pace with evolving threats. But despite fast moving events and rapid development in techniques, the target of most cyber attacks remained people. And people remain the best foundation for building a resilient defense.

Here’s what we suggest as a starting point:

- ☑ **Train users to spot and report malicious email.** Regular training and simulated attacks can raise awareness of attacks and help identify people who are especially vulnerable. Look for solutions that use real-world attack trends to model their simulations.
- ☑ **Manage access to sensitive data and insider threats.** A cloud access security broker can help secure cloud accounts and ensure the right levels of access are granted to users and third-party apps. Insider risk management platforms can help protect against insider threats, including users compromised by external attacks.
- ☑ **Partner with a threat intelligence vendor.** Focused, targeted attacks call for advanced threat intelligence. Leverage a solution that combines static and dynamic techniques to detect new attack tools, tactics and targets—and then learns from them.
- ☑ **Start with people.** Email and the cloud are today’s primary attack vectors. Manage threats with an intelligent, holistic and people-centric approach that blocks attacks, secures cloud accounts and educates users.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.