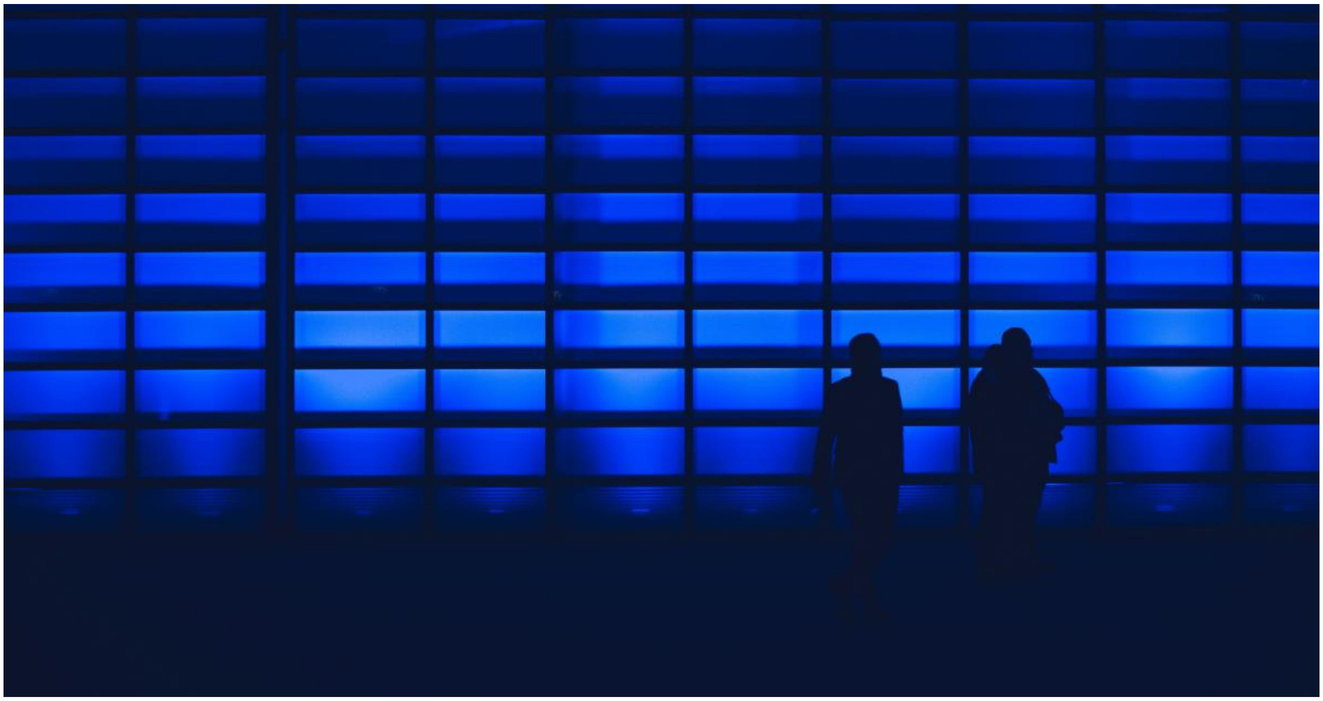
Q4 2020 Threat Report | Proofpoint US

proofpoint.com/us/blog/threat-insight/q4-2020-threat-report-quarterly-analysis-cybersecurity-trends-tactics-and-themes

February 12, 2021



Security Brief: Q4 2020 Threat Report: A Quarterly Analysis of Cybersecurity Trends, Tactics and Themes

In today's threat landscape, people are the new perimeter. Whether it's malware, email fraud, cloud account takeover or credential phishing, cyber attacks no longer focus on breaking through network controls and cracking technical flaws. Instead, they target users and exploit human nature.

That’s why people are at the center of our cybersecurity mission—and why user-activated attacks are the focus of this report. Like most threat reports, this one highlights the latest quarter’s attack trends, campaigns and themes. But it goes a step further, exploring how attackers target people and what you can do about it.

Our goal in this report is twofold. First, we want to help demystify cybersecurity by shedding light on the people-centric nature of today’s threats. Second, and just as critical, we want to show how organizations can use this insight better protect their greatest asset and today’s biggest risk: their people.

The report is a small slice of the insight we offer customers through the Proofpoint Nexus Threat Graph. Every day, we analyze billions of email messages, billions of URLs and attachments, tens of millions of cloud accounts and more—trillions of data points across all the digital channels that matter. Our global footprint and laser focus on people-related cyber risk give us a unique view into today’s biggest cyber threats.

Except where noted, this report covers threats and threats observed directly by our global network of threat researchers.

Top attack techniques

Email is by far the biggest channel for cyber attacks. We saw a wide range of email attack techniques in the fourth quarter, but almost all of them included some form of social engineering.

The term “social engineering” can include any number of psychological techniques that trick people into doing something the attacker wants them to do. That may mean opening a malicious attachment, clicking on an unsafe URL, sending login credentials or sensitive information or even wiring money to the attacker.

Figure 1 shows attacks that used social engineering in tandem with a technical exploit or technique. In many cases, social engineering is used to trick users into doing something directly—no malware needed. If listed as a separate technique, social engineering would easily dominate the chart as a component in 99% of all attacks.

When used with a technical exploit, social engineering might be something as simple as creating a hard-to-resist subject line, spoofed email address. In other cases, it might be as involved as impersonating a trusted colleague to lure new victims.

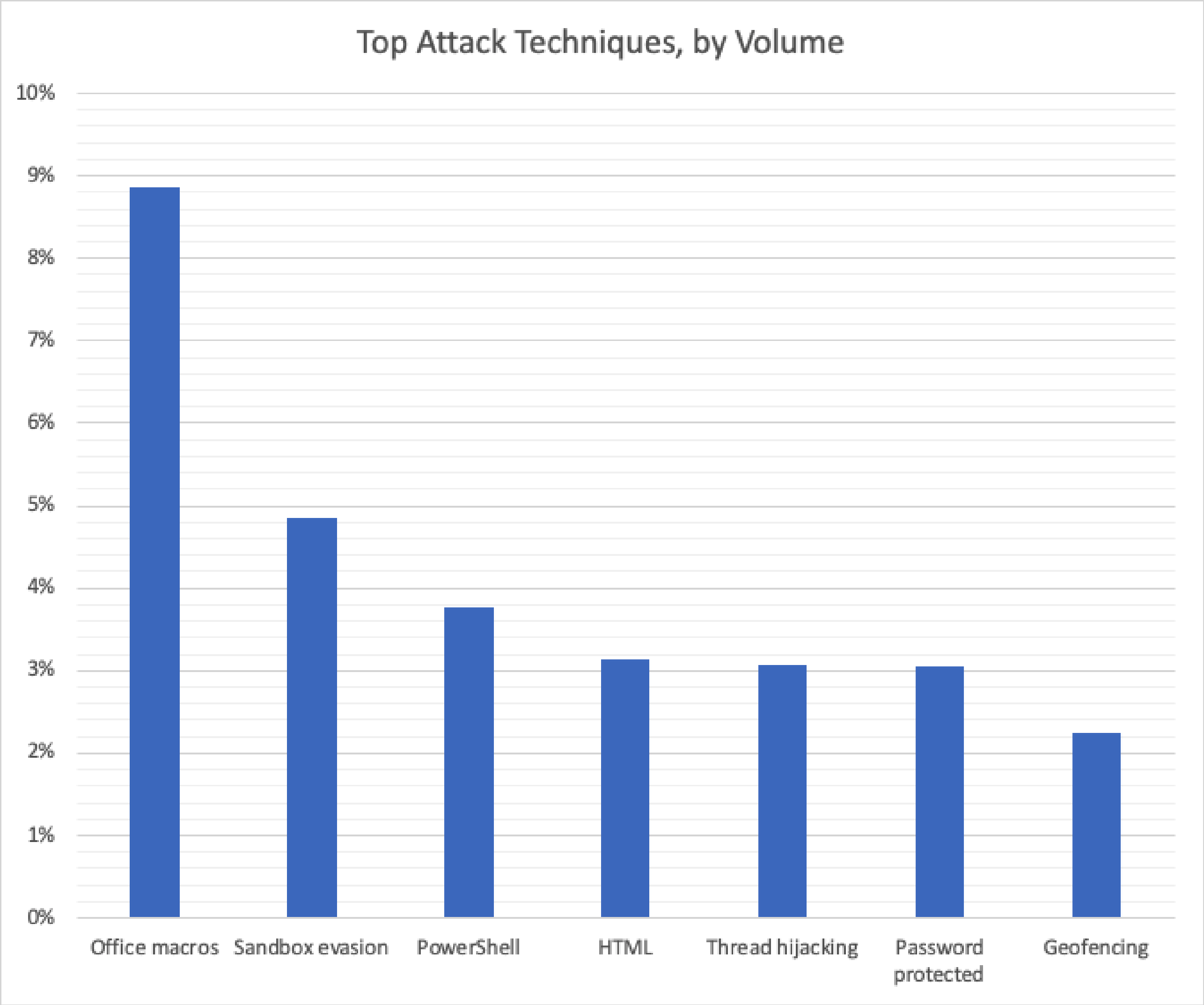


Figure 1

Here's a summary of how these techniques work:

- **Office macros:** Exploits flaws in a mini-programming language designed to help automate and extend Microsoft Office features. Attackers use it to create embed malicious macros that infect users' device when opened. Most attacks involve tricking the user into not just opening the document but enabling macros. Many recent attacks feature a new twist on a decades-old feature of Excel. These are often classified as Excel 4.0 (XL4) attacks.
- **Sandbox evasion:** Modern threat-detection tools safely "detonate" unknown files within virtual machine settings to see what they do when clicked or opened. Sandbox evasion techniques can prevent the malware from running or limit telltale behaviors in virtual environments to avoid being discovered. One of the big evasion techniques we saw in Q4 was using Windows' Regsvr32 command line tool in a way that is not detected within most sandboxes. (Regsrv32 was designed to help PC administrators, but it can be exploited to let attackers bypass Windows' AppLocker security tool.)

- **PowerShell:** Exploits Windows' built-in administration tool to infect victim's PCs. These attacks usually start with a phishing email that includes a URL that links to a page with embedded code that uses the PowerShell feature to take over the victim's machine. These attacks are hard to detect because they use a legitimate Windows feature and don't start with a full malware file. The feature can also be used to download and run other malicious files from the internet.
- **HTML:** Web pages can include all kinds of code that exploits flaws in popular browsers and, on rare occasions, operating systems. These include legitimate but compromised websites and web-based ads. Most attacks that use this technique trick the victim into clicking an unsafe URL, but attackers can also send HTML pages directly through email.
- **Thread hijacking:** After taking over someone's email account, the attacker contacts people the compromised user knows, replying to past and ongoing email threads with a malicious email.
- **Password protected:** Adding password protection to a malicious file can lock it away from many malware-detection tools. The attacker gives human readers the password and tricks them into opening and unlocking the file.
- **Geofencing:** Limits malware behaviors to defined geographies using the infected device's GPS and other location features. This technique is used to target attacks or evade detection tools.

Top Threat Actors:

Among malicious emails we could tie to a known threat actor, more than 60% of the total volume we saw in Q4 came from just two attackers, which we have designated as TA544 and TA542 (also known as Emotet). Both attackers were also among the most prolific threat actors in Q3.

Note: This charts highlights email attacks that we could confidently tie to a known threat actor. Determining who is behind an attack, a process known as attribution, is not always possible. The cyber criminal ecosystem is vast and highly fragmented. Unattributed attacks are not included in this chart to analyze and compare the biggest threats.

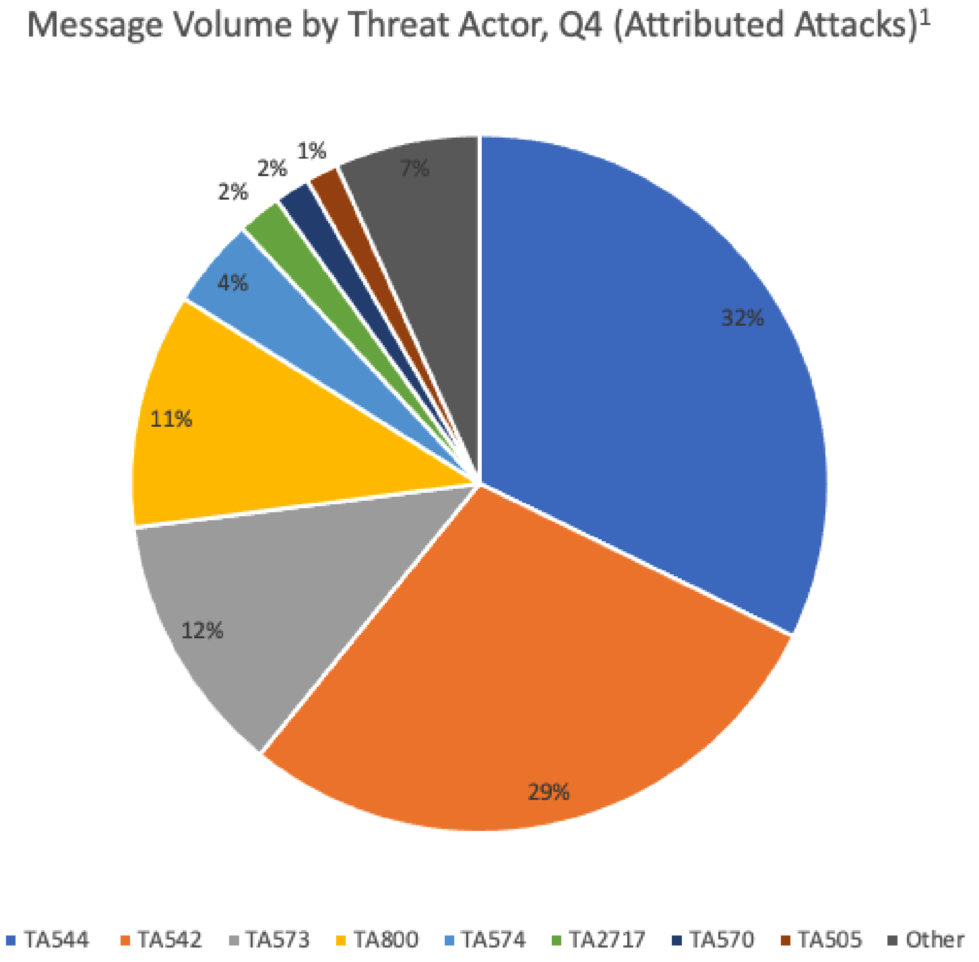


Figure 2

What are ‘threat actors?’

Threat actors is a term threat researchers use to describe an attacker or groups of attackers. They can include:

- **State-sponsored attackers**. Also known as advanced persistent threats (APTs), these attackers typically engage in espionage on behalf of a government. But attacks may also involve intellectual property theft, outright financial theft and attacks designed to disrupt or damage data and systems. Whatever approach they take, they’re all meant to achieve a military or diplomatic goal.

- **Cyber criminal rings**. These organized crime groups are usually in it for the money. In many cases, they work like multilevel marketing franchises. An advanced threat actor creates the malware "product" and sets up the infrastructure as an easy-to-use package or service. Lower-level cyber criminals may rent the service for their attacks, paying to use it for a set period of time or getting a cut for each successful compromise. In other cases, they act as distributors, sending out emails with the malware and earning a commission on each successful infection. Some researchers consider the most advanced cyber criminal groups to be APTs.
- **Hacktivists**. This portmanteau of "hacking" and "activism" refers to attacks meant to make a political statement or effect policy change. These attacks, though rare, typically expose secret information, disrupt perceived wrongdoing or embarrass foes. While their goals are different, they use many of the same tools and techniques as other types of attackers and can cause just as much harm.

Knowing who is behind an attack—and what their motivations are—can be a critical part of defending against them.

TA542 and the demise of Emotet

TA542 has become one of the most prolific in recent years due to massive campaigns that use a malware strain called Emotet. The group has targeted multiple industries around the world, sending hundreds of thousands—or even millions—of messages per day.

Dubbed "the world's most dangerous malware,"[1]Emotet is versatile and highly adaptable. It was first discovered in 2014 as a simple banking Trojan aimed at stealing account credentials. Since then, it has evolved into a highly versatile malware strain used for everything from stealing data to harvesting email to ransomware. Emotet has been used to target critical industries around the world, including banking, e-commerce, healthcare, academia, government and technology.[2]

Emotet doesn't just compromise the systems they infected. It also uses these compromised machines to launch new attacks, absorbing them to a zombie-like network of more than a million similarly infected machines known as a botnet. Other cyber criminals can pay TA542 to use the botnet for all kinds of attacks—or could until just a few weeks ago.

The takedown

Authorities said in late January that they had shut down Emotet's infrastructure as part of a coordinated effort across nine countries in North America and Europe.[3] Law enforcement appears to have taken over all three of Emotet's known botnet networks. Authorities plan to retool the botnets to remove its own malware from infected systems.[4]

What's next?

At this stage, there's no telling what Emotet takedown means over the long term. TA542 had remained active in the days leading up to the shutdown, and efforts to disrupt large botnets in the past have had mixed results. We don't know how large the team was operating the Emotet botnet and whether all of its members were in the Ukraine, where at least two of Emotet's operators were arrested.[5]

If segments of the botnet and associated operators survive, Emotet's source code may be retooled under a new infrastructure and new moniker. Threat actors often build redundancy into their infrastructure, and their teams often live in countries beyond the reach of the law.

TA544 goes on a financial cyber crime spree

First documented in 2017, TA544 is part of a financial crime ring that has targeted a range of industries Japan and several European countries, with a heavy focus on manufacturing and tech firms. It is an affiliate that distributes several strains of malware, including Panda Banker and others.

A large share of its attacks use a Trojan called Ursnif, but it's not clear whether it controls Ursnif or is just one of the groups using it. The malware stems from leaked source code and is used by many other threat actors.

One of TA544's distinctive traits is how is uses steganography, hiding malicious code in seemingly benign images.

TA573: a top-tier distributor with ties to Evil Corp

Like other illicit markets, cyber crime is a loose, multilayered ecosystem that includes suppliers, distributors, money launderers and other specialties. TA573 operates as a malware "affiliate," which sends malware someone else has created.

Think of affiliates as the last mile of the malware supply chain. They don't write malware or run the infrastructure used to support attacks. Instead, they're the malware distributor, selecting targets and crafting emails designed to trick recipients into engaging with them. Cyber criminals' business models vary, but affiliates typically get a commission on every victim infected.

TA573 is an affiliate distributor of Dridex, a malware strain that resurged in 2020 after a lying low through most of 2019. The malware itself is a creation of a Russian cyber crime group that calls itself Evil Corp,[6] a longtime menace that recently turned to ransomware.[7] In June, U.S. authorities offered $5 million for information leading to the arrest of Evil Corp's operators, the largest reward ever for a cyber criminal.

TA800 holds healthcare data hostage

This attacker is an affiliate distributor of the The Trick, also known as Trickbot, and BazaLoader. (For more on how affiliates work, see the description of TA573).

TA800 has targeted a wide range of industries in North America, infecting victims with banking Trojans and malware loaders (malware designed to download other malware onto a compromised device). Malicious emails have often included recipients' names, titles and employers along with phishing pages designed to look like the targeted company. Lures have included hard-to-resist subjects such as related to payment, meetings, termination, bonuses and complaints in the subject line or body of the email.

In Q4, it was responsible for a wave attacks against the healthcare sector using a loader called BazaLoader. BazaLoader, under the control of a separate threat actor, subsequently installed a ransomware strain called Ryuk. (Some researchers believe BazaLoader was created by the same malware team behind The Trick—in part because both malware strains infected victims with Ryuk.)

Ransomware encrypts data on infected devices, effectively locking victims out of their data and systems until they pay the attacker to regain access.

Healthcare organizations have become an especially enticing target for ransomware attacks. They are often not as well protected as other sectors and the life-and-death nature of the business means they can afford little downtime.

Three U.S. government agencies warned hospitals in October of an “increased and imminent” cyber crime threat that included ransomware attacks.[8]

TA574: a new entrant draws on legacy malware

A relative newcomer, TA574 appears to be another affiliate focused on malware distribution. (For more on how affiliates work, see the description of TA544).

TA574 has launched attacks against a wide range of industries, sending an updated version of 15-year-old banking Trojan called Zloader. It's an offshoot of the infamous Zeus banking Trojan, which has been used to steal millions of dollars from victims' banking accounts.

The group also uses Ostap, a malware downloader that uses JavaScript to hide itself from security sandbox analysis tools (see the “Top Attack Techniques” section for more on sandbox evasion).

Attribution: the known unknowns

As noted earlier in this section, Figure 1 includes only attacks that can be tied to a known threat actor. This focus is helpful but may make the universe of attackers seem more concentrated than it actually is.

As Figure 2 shows, nearly 90% of campaign-related email volume we saw in Q4 can’t be attributed to known attackers. (That figure is even higher for email that is not part of a campaign.)

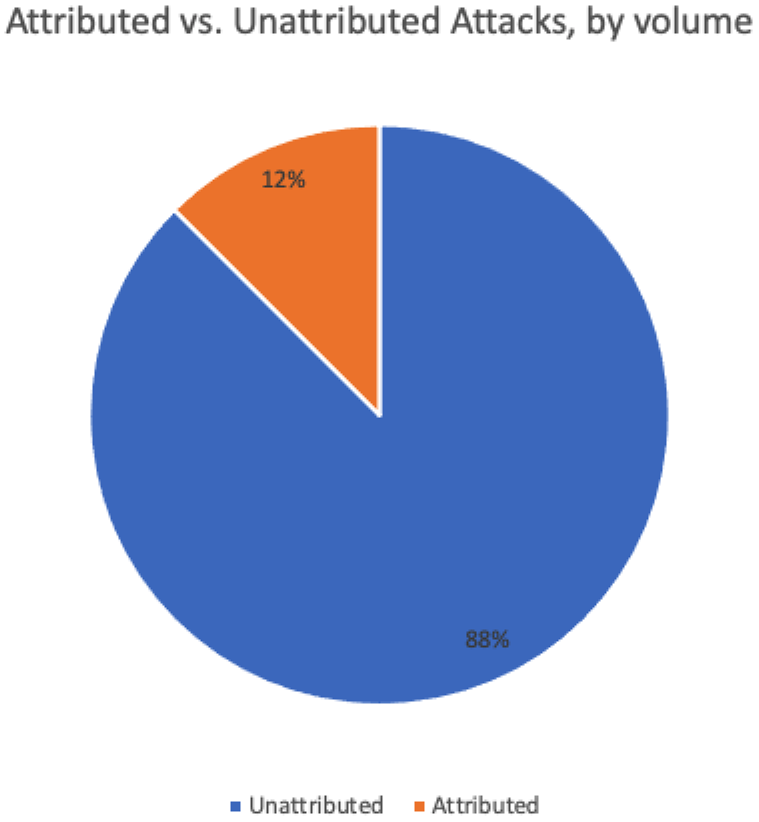


Figure 3

It’s easy to see why. Would-be hackers with little technical skill can easily access the malware and infrastructure they need for successful campaigns, greatly lowering barriers to entry. And as explained in the last section, many attacks don’t require these tools at all—just a keen understanding of human nature and a knack for persuasion.

It’s a testament to the breadth and diversity of today’s threat landscape—and a reminder that organizations looking to protect their users, data and systems must be prepared for anything.

Conclusion and Recommendations

Today’s attacks target people, not infrastructure. That’s why you must take a people-centric approach to cybersecurity. That includes user-level visibility into vulnerability, attacks and privilege and tailored controls that account for individual user risk.

Here’s what we recommend as a starting point.

- **Train users to spot and report malicious email**. Regular training and simulated attacks can stop many attacks and help identify people who are especially vulnerable. The best simulations mimic real-world attack techniques. Look for solutions that tie into real-world attack trends and the latest threat intelligence.
- **At the same time, assume that users will eventually click some threats**. Attackers will always find new ways to exploit human nature. Find a solution that spots and blocks inbound email threats targeting employees before they reach the inbox. Invest in a solution can manage the entire spectrum of email threats, not just malware-based threats. Some threats—including business email compromise (BEC) and other forms of email fraud—can be hard to detect with conventional security tools. Your solution should analyze both external and internal email—attackers may use compromised accounts to trick users within the same organization. Web isolation can be a critical safeguard for unknows and risky URLs.
- **Manage access to sensitive data and insider threats.** A cloud access security broker can help secure cloud accounts and help you grant the right levels of access to users and third-party add-on apps based on the risk factors that matter to you. 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 at scale to detect new attack tools, tactics, and targets—and then learns from them.

[1] Europol. “World’s Most Dangerous Malware Emotet Disrupted Through Global Action.” January 2021.

[2] U.S. Department of Justice. “Emotet Botnet Disrupted in International Cyber Operation.” January 2021.

[3] Danny Palmer (ZDNet). “Emotet: The world's most dangerous malware botnet was just disrupted by a major police operation.” January 2021.

[4] Catalin Cimpanu (ZDNet). “Authorities plan to mass-uninstall Emotet from infected hosts on April 25, 2021.” January 2021.

[5] Andy Greenberg (Wired). “Cops Disrupt Emotet, the Internet's ‘Most Dangerous Malware.’” January 2021.

[6] Krebs on Security. “Inside ‘Evil Corp,’ a $100M Cybercrime Menace.” December 2019.

[7] BBC. “Russian hacker group Evil Corp targets US workers at home.” June 2020.

[8] Nationals Cyber Awareness System. “Alert (AA20-302A): Ransomware Activity Targeting the Healthcare and Public Health Sector.” October 2020.