KROLL

Q3 2021 Threat Landscape:

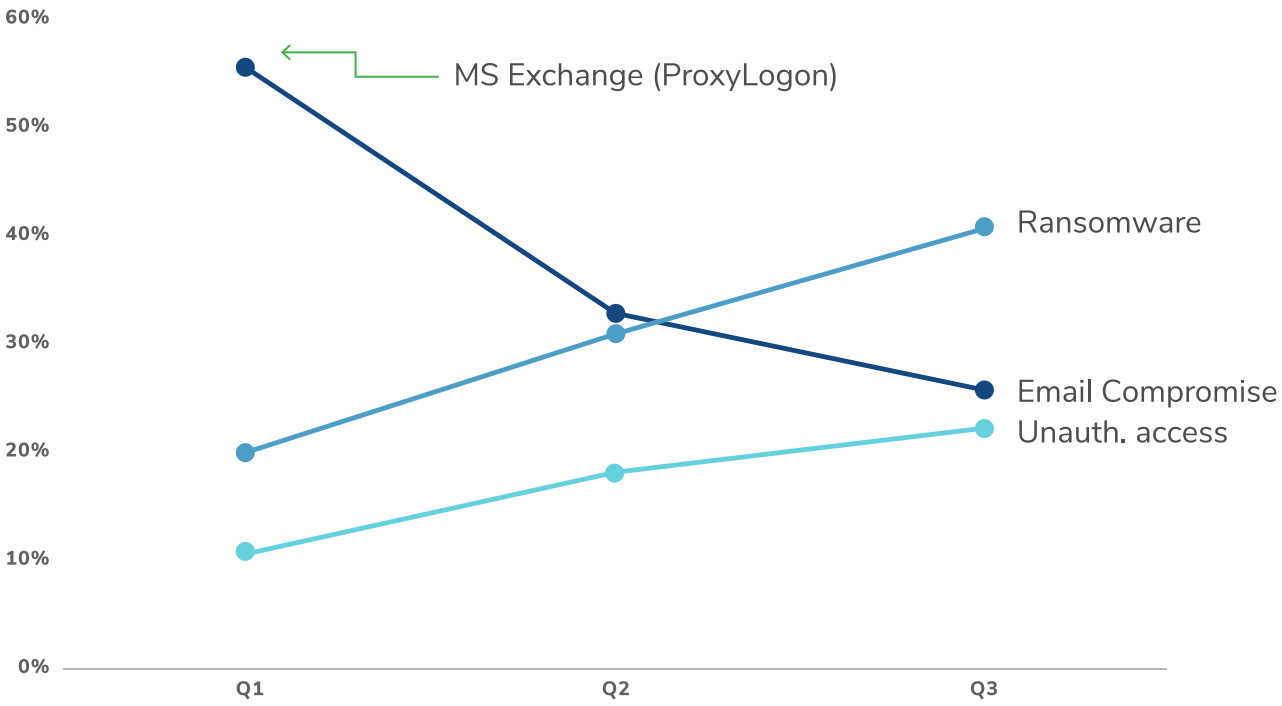
Ransomware in the Supply Chain

Q3 2021 Threat Landscape: Ransomware in the Supply Chain

— Authors: Keith Wojcieszek, Laurie Iacono, Thomas Brittain, Amanda Haddan

In a pattern of continued growth across the third quarter of 2021, ransomware remains the dominant threat type, more than doubling since 2021 Q1, fuelled by an exponential increase in the initial access broker marketplace. Incidents of unauthorized access and the risk of insider threats also increased, but to a far lesser extent, accounting for roughly 20% of incidents in the same period.

Most prominent threat incident attack methods 2021 (% of total)



Supply chain attacks have been on the rise in Q3 as ransomware actors seek to organize their attacks to take advantage of third-party vulnerabilities in supply chains, giving them easy access to hundreds of potential victims. The use of initial access brokers, who rapidly exploit recently announced vulnerabilities to sell access to the highest bidder, is also increasing among ransomware groups, demanding greater visibility and faster response from cyber teams.

Q3 Threat Timeline

Jul 2 **REvil** attacks Kaseya's Virtual System Administrator resulting in the compromise and encryption of data belonging to hundreds of client businesses. Several service providers with client businesses of their own were consequently impacted by the incident

Jul 13 **Revil** leak site, "Happy Blog" taken down using compromised backups

Jul 16 Microsoft PrintNightmare critical vulnerability patched, ransomware groups quickly adopted it for attacks

Jul 23 The since-disbanded BlackMatter gang begins "big game" hunting, targeting companies with revenues of more than U.S.$100 million and actively recruiting new members and affiliates

Aug 5 A disgruntled ex-affiliate of the **Conti** ransomware program leaked the manuals and guides used by the Conti gang to teach affiliates how to gain access to a company, move laterally, and then exfiltrate data before encrypting files

Aug 11 Following its appearance in June, Lockbit 2.0 begins to gain "marketshare" after DarkSide and REvil shut down and successfully compromises a growing number of organizations

Sep 3 A spate of government-targeted attacks begins with the French government announcing its visa website had been subject to an attack exposing applicants' personal data. This was shortly followed by a DDoS attack on the New Zealand postal service and several of the country's financial institutions, and a ransomware attack on South Africa's Department of Justice and Constitutional Development by the hacking group **CoomingProject**, which took all electronic services offline

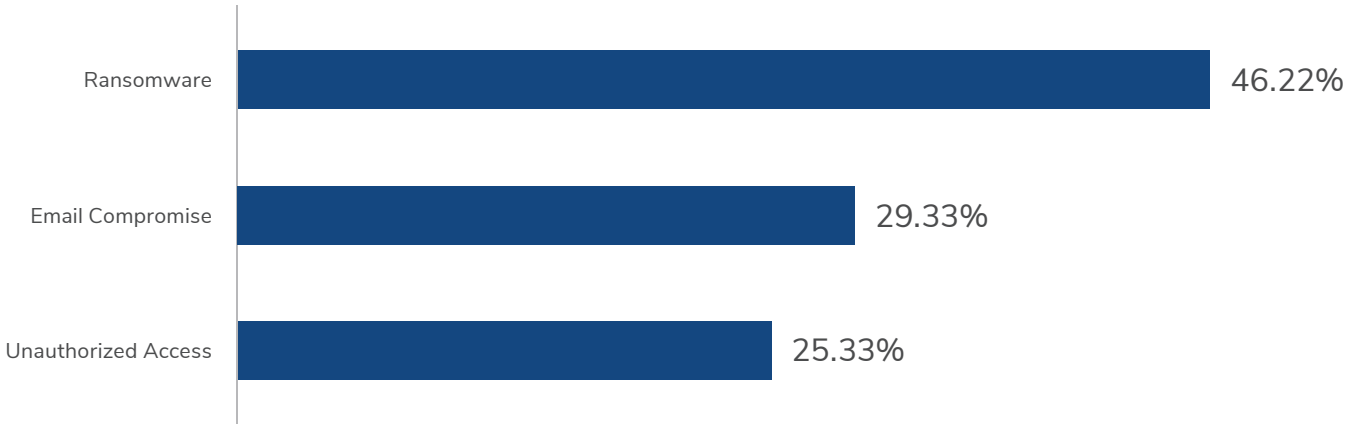
Sep 7 **Revil** resurfaces and "Happy Blog" site reappears

Mid-Sep A new malware loader known as Squirrelwaffle identified in new attack chain used to deliver Cobalt Strike, which enables adversaries to execute further malware, often preceding ransomware attacks

Such incidents are worth highlighting as they dramatically increase the risks facing organisations and alter the landscape in which businesses operate, particularly with CVE and zero-day exploitations now accounting for one in six (12%) infection vectors.

Q3 Threat Timeline

Most prominent threat incident attack methods Q3 (% of total)



In Q3, we saw ransomware continue to dominate as the most prominent method of attack. Increasing by over 11% on the previous quarter, its share of total incidents has more than doubled this year from 20% in Q1 to around 46% in Q3, giving cyber teams very real cause for concern.

> **“Ransomware remains a huge threat to organizations of all shapes and sizes. We’ve seen threat actors mobilize and expand their efforts since the beginning of the pandemic, and incidents like the Conti leak only serve to democratize the methods used by cybercriminals to gain access to businesses. An ounce of prevention is worth a pound of cure when it comes to ransomware, so we encourage all businesses to constantly evaluate the security controls they have deployed rather than waiting for an incident to occur”**
>
> — Devon Ackerman, North America Practice Lead, Cyber Risk

Surprisingly, given the recent trend toward remote working, business email compromise (BEC) was down by nearly 4% on Q2's figures. BEC nevertheless remains a major threat for cyber teams, accounting for almost 30% of all attack vectors.

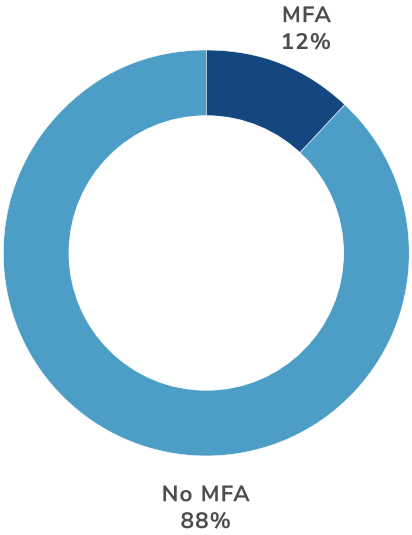
Cases of unauthorized access, increasingly common among healthcare HIPAA privacy and security violations, accounted for around 25% of all incidents in Q3, up by 7% from Q2.

> **"Ransomware actors are opportunists. Nothing demonstrates this more clearly than the exponential increase in initial access brokers which has enabled ransomware criminals to scope out potential targets across a vast field of opportunity as brokers compromise organisations at scale. While some businesses are most certainly targeted, all businesses are potentially vulnerable."**
>
> — Elaine Hung, Vice President, Cyber Risk

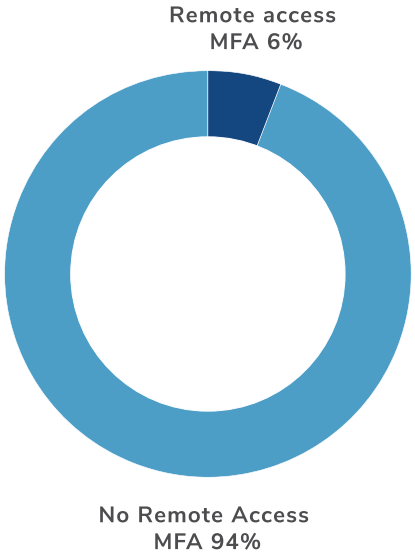
Multi-Factor Authentication is Still Critical

In all incidents recorded in Q3, victims had multi-factor authentication (MFA) in place in only 11.5% of cases and only 5.7% of cases had remote access MFA.

All incidents Q3



All incidents Q3



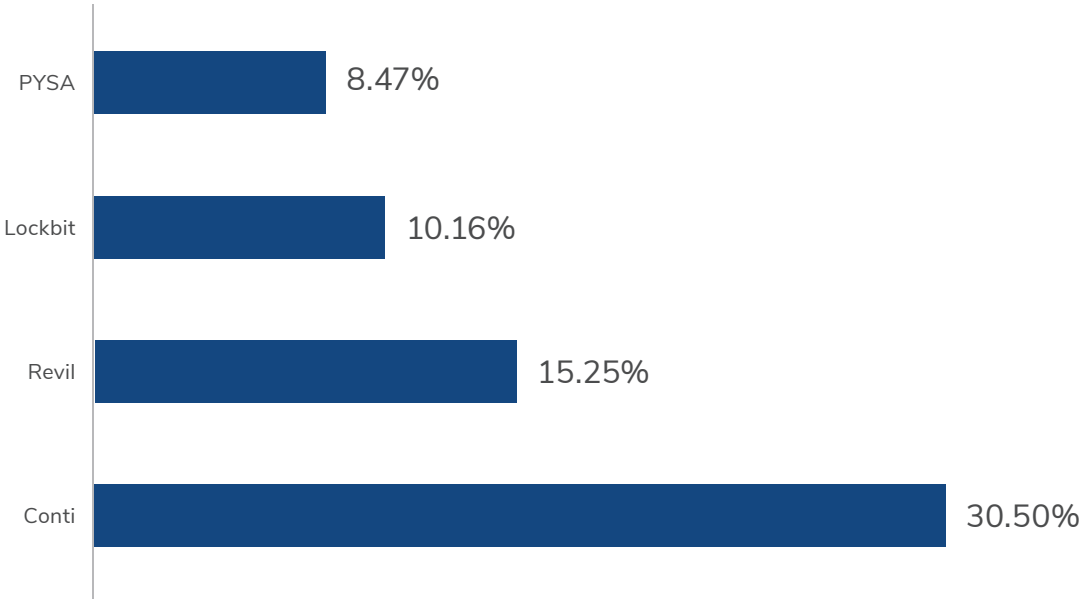
It's concerning that MFA technology by and large is not currently in use by businesses being targeted by malicious actors – MFA and other authentication technologies are crucial in the fight against attacks.

> **"Using strong identity protection such as multi-factor authentication is often the best step a business can take to protect itself in terms of outlay and reward. It's relatively simple to set up and can prevent an overwhelming majority of attacks. As we can see from the Q3 data, a large majority of victims were businesses that did not have fully implemented MFA in place."**
>
> — Mari DeGrazia, Associate Managing Director, Cyber Risk

Threat Actor Groups Continue to Grow

The **Conti** ransomware group remained the largest threat actor in Q3, accounting for more than 30% of all incidents, up nearly 7% from Q2. The group has developed a reputation for targeting hospitals, 911 dispatch carriers and other emergency medical services with potentially life-threatening consequences. To date, **Conti** has been connected to more than 400 cyberattacks against organizations worldwide with demands as high as U.S.$25 million.

Most prominent threat actor groups Q3 (% of total)



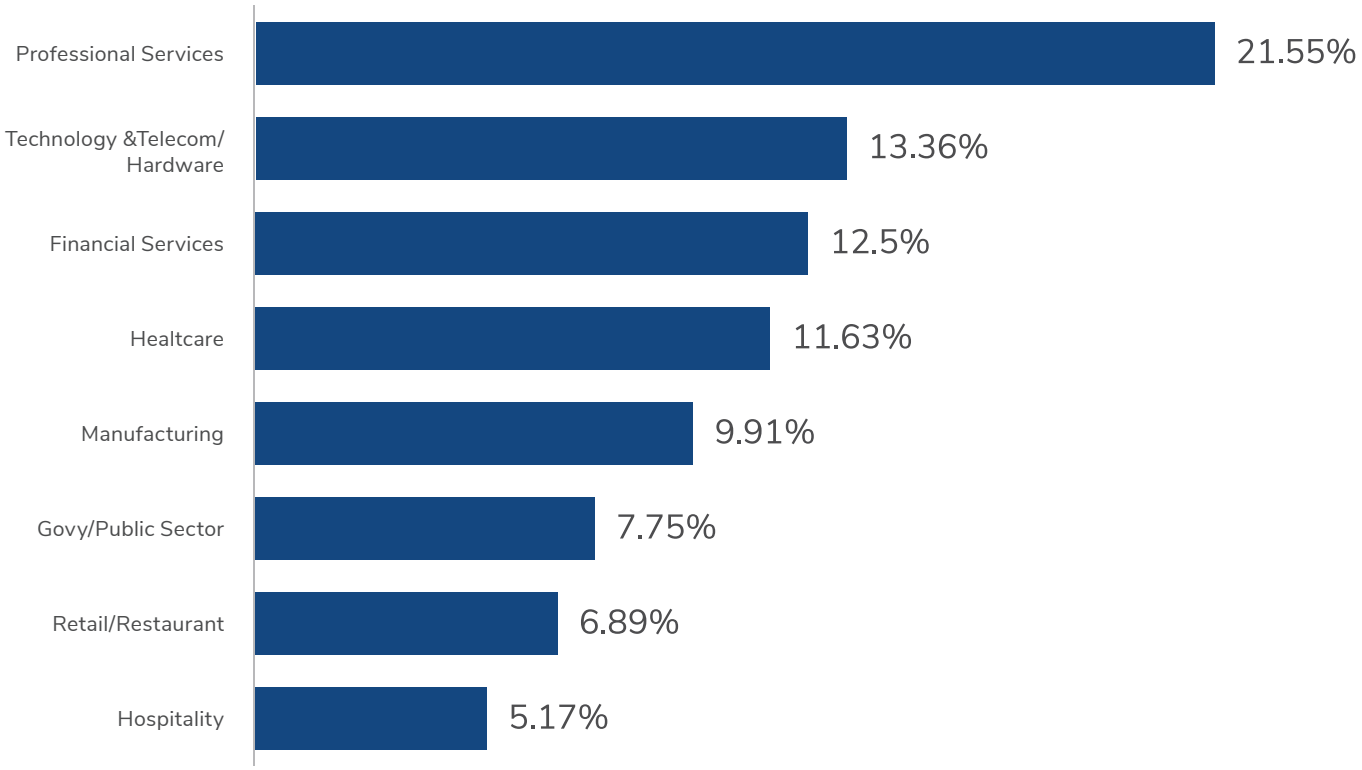
The **REvil** group is the second most prominent threat actor in Q3, responsible for more than 15% of ransomware incidents, down 2.4% from Q2. The **Lockbit** and **PYSA** groups are both gaining traction, up 5.8% and 2.6% on last quarter's incident figures respectively.

Since its first attack in September 2019, **Lockbit** has continued to be one of the most advanced lockers on the market, focusing on the speed of encryption as well as functionality. In June 2021, the R-a-a-S group announced recruitment for their affiliate programme, **Lockbit 2.0**, following attacks that surged in Q3. The group enables affiliates to automatically access victims' networks using easy to procure valid remote desktop protocol credentials. Then, it provides them with a Trojan called **StealBit**, which steals data from victims' networks, according to researchers at security firm Trend Micro.

Professional Services Sector Suffers the Biggest Q3 Blow

The professional services sector remained the most targeted sector overall in Q3, increasing its lead by nearly 4% on last quarter's figures. This is most likely due to attackers increasingly utilizing supply chain breaches to reach as many victims as possible in a single attack.

Most targeted sectors Q3 (% of total)



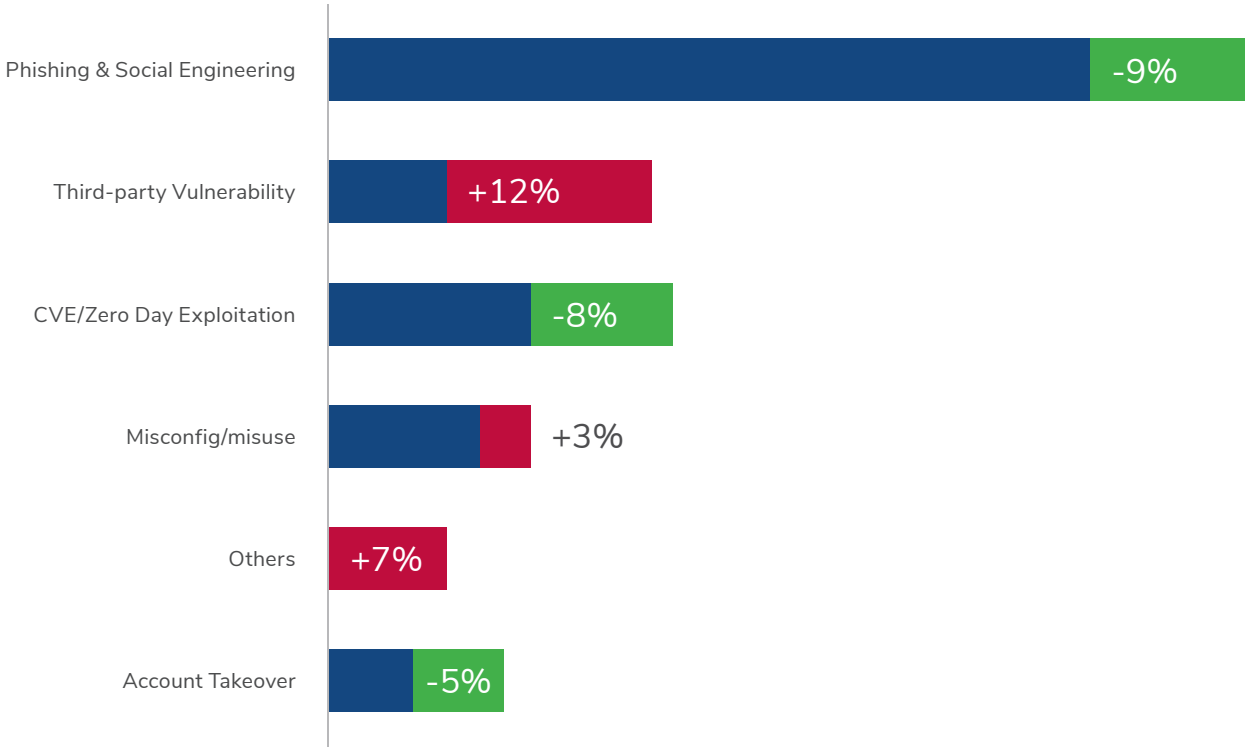
State of play: what are the risks facing businesses in 2021 Q3

The pandemic continues to have a profound impact on businesses. In some instances, organizations have benefited from the accelerated pace of digital change, enhancing productivity, and broadening their talent pools. Such progress has not come without risk, however.

Threat actors have continued to weaponize the pandemic and use it as an opportunity to hit vulnerable businesses as they move more of their operations online. Attack surfaces have proliferated rapidly, making the work of security teams more challenging, and the evolution of the initial access broker market has further democratized ransomware for threat actors with resources. In terms of vectors for infection, perhaps the most striking thing about Q3 is that third-party vulnerability exploitation is up 12% on the previous quarter.

It's also worth noting that the implications of cyber threats create other risks – namely, around bribery and corruption. According to Kroll data, of the 46% of firms who expect ABC risks to increase in 2022, half attribute this to cybersecurity and data breaches.

Most prominent infection vectors Q3 (% of total)



Initial access brokers fuel ransomware in Q3

Initial access brokers are threat actors that carry out 'reconnaissance' on potential victims, identifying vulnerable networks or those with vulnerable applications. Vulnerabilities quite often come in the form of virtual private network (VPN) appliances with exposed software weaknesses, or remote desktop protocols (RDPs), both of which have become more common since the beginning of the pandemic. Once an initial access broker has access to a network, it then sells access to ransomware operators and affiliates on the dark web. The rise of initial access brokers could explain why CVE exploits are among the most common infection vectors this quarter, and why ransomware continues to further its lead as the number one incident type.

Lack of MFA still a boon for threat actors

An overwhelming majority of ransomware victims in Q3 didn't have multi-factor authentication (MFA) in place. MFA strengthens security by not only requiring a username and password to log in, but also a one-time code sent to a phone or an authenticator app. These are simple measures which, unfortunately, not enough businesses are deploying. Regular patches and updates can only do so much; the rest lies with preventative measures such as MFA and the use of strong, unique passwords, among other key steps every organization should take.

MFA is not a silver bullet for email account protection

Kroll has worked recent investigations in which threat actor groups leverage social engineering, combined with phishing, as a strategic method in overcoming MFA protections. Threat actor groups can accomplish this by selecting the phone call verification method that is an option for accessing email accounts in Microsoft 365. The victim then receives the MFA verification phone call from a legitimate Microsoft phone number and often times, unknowingly selects the pound (#) sign to approve the access request.

Unfortunately, this is exactly what the threat actor is counting on, unintentionally authenticating access for the threat actor(s) and adding the requesting device to the account's trusted devices list in the Microsoft 365 tenant. If MFA is configured with "Remember Multi-Factor Authentication," companies should be aware that it allows users to disable MFA temporarily on trusted devices for a configured, limited number of days. If the threat actor has accomplished this, then their device will become trusted for the timeframe usually needed to search emails, set up mail rules, and craft a fraudulent wire transfer or some other type of targeted attack process.

Incidents of unauthorized access on the rise

Unauthorized access incidents such as the misconfiguration of cloud systems and insider threats also grew from Q2 to Q3. Insider threat-related cases in particular have seen an increase with a lot of dark web and open source activity throughout the quarter. Threat actor group **Lockbit** contributed to the insider threat problem by actively attempting to recruit employees to assist in attacks, in some cases offering large pay-outs. **Lockbit 2.0**, the gang's new ransomware-as-a-service tool launched in June, even changes the desktop wallpaper on encrypted devices to a message offering "millions of dollars" for the credentials of corporate insiders.

Remote access trojan malware wreaks havoc

Active in Q3, threat actor group **PYSA** is known for deploying a GO-lang remote access Trojan malware to maintain backdoor access to sensitive data. In Q3, another group known as **Hive** used a ransomware strain written in Go-lang to attack multiple different healthcare organizations. GO is attractive to malicious actors largely because it's open-sourced and is hard to reverse engineer, meaning there are fewer detection techniques. Malware written in GO is more likely to evade monitoring - something cyber teams will need to bear in mind moving into Q4 and beyond.

Professional services sector hit hardest

There weren't any significant changes at the top end of the sectors targeted by malicious actors in Q3, with professional services and healthcare continuing to be aggressively pursued. Professional services was the most attacked sector by a significant margin, probably owing to companies' increased dependency on managed service providers and their trusted connections to clients. Government and public sector targeting was also up by nearly 5% on the previous quarter, significant because it indicates a change in strategy from malicious actors who had refrained from these targets during the pandemic.

Constant Change, Relentless Pressure In Q3

Security teams around the world are continuing to rise to the challenges brought about by the pandemic, but the relentless pressure these teams have been under is showing no signs of easing as we near the end of 2021. The threat landscape is continually changing, shown by the disbanding of one Q3's most prominent threat actors, BlackMatter. The group announced in November that it would shut down due to increased pressure from authorities, and speculation is rife that a team member may have been arrested. Even more recently, law enforcement in the U.S. and Europe announced a series of actions aimed at the REvil group, designed to combat what President Biden called "a prime national security threat". Encouragingly, this is a sign that the fightback is in progress.

Businesses that have demonstrated their ability to adapt and perform under new working conditions need to harness that same energy when it comes to their security practices. Prevention is always better than cure, and the time has never been better for teams to re-evaluate their detection and response capabilities, start using MFA and other best practices, and assess the integrity of their maturing supply chains. Inundated security teams might also benefit from third-party support when it comes to the detection and containment of threats, augmenting their own in-house expertise and adding in new forms of security automation.

KROLL

About Kroll

Kroll provides proprietary data, technology and insights to help our clients stay ahead of complex demands related to risk, governance and growth. Our solutions deliver a powerful competitive advantage, enabling faster, smarter and more sustainable decisions. With 5,000 experts around the world, we create value and impact for our clients and communities. To learn more, visit www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Duff & Phelps India Private Limited under a category 1 merchant banker license issued by the Securities and Exchange Board of India.