Threat actors are exploiting the growth of QR codes by sending out targeted phishing emails containing malicious codes

LOOKING BACK TO MOVE FORWARD

How the teachings of the past year can be used to bolster security in 2022

If 2021 has taught the security industry anything, it's that we're still far away from reducing the impact of ransomware attacks. Initial access points to networks pervade the internet and threat actors exploit them using three primary techniques. Firstly, via email-based attacks, with phishing being the principal attack vector; secondly, through password-based attacks, where weak and easily guessable passwords that are often used more than once, and shared between cyber criminals are exploited; and finally through vulnerabilities where outdated and exposed assets are found and targeted.

Sophisticated attackers will always exploit our ever-changing circumstances to maximise their own profitability, meaning it is imperative to prioritise combative measures when it comes to preventing your organisation from becoming the next big ransomware headline in 2022.

With ransomware attacks continuing to grow in popularity among the cybercriminal community, security experts consider the implications this attack vector will have on organisations in the coming year. As well as detailing the tried-and-tested methods already mentioned, many look at the cunning new techniques threat actors are expected to harness for ransomware attacks.

Read on to equip yourself with knowledge from industry experts on how to best combat the tools in an attacker's ransomware arsenal.

ED WILLIAMS, DIRECTOR OF TRUSTWAVE SPIDERLABS EMEA:

"We've got a long way to go when it comes to reducing the impact of ransomware. Initial access points like exploiting vulnerabilities are still pervasive across the internet. We've seen an uptick in the use of remote access solutions, like VPNs, but we've also seen an uptick in their lack of security hardening, allowing malicious threat actors/ransomware access to internal infrastructure. Ensuring that all internet-facing infrastructure is security tested should be a priority to reduce the risk of a ransomware attack.

We are still seeing weaknesses within infrastructures. We have a 100 percent success rate of gaining domain authority during our security testing engagements. Admittedly, this isn't always the best metric for measuring security across organisations, but it does demonstrate that should ransomware or a malicious threat actor gain access, then the ability to move laterally and escalate privileges is likely.

The key to defending against ransomware attacks is making sure that good cyber hygiene is enforced across the enterprise, which is challenging to enforce in reality. Basic cyber hygiene should be every organisation's focus moving into 2022."

ANDREW RUBIN, CEO AT ILLUMIO:

"2022 will be all about ransomware… again. All crimes, including ransomware attacks, are done for one of two reasons: one, as a political statement or two, for money. In 2021 we saw that ransomware can be both wildly successful and devastating (ie, the attacks on Colonial Pipeline and Kaseya), in part because adversaries found a way to be highly efficient in their attacks – they can keep costs low and take advantage of a repeatable operating model. Because this model has become so effective, malicious actors will only accelerate their focus on ransomware in 2022.

While ransomware is here to stay, there are ways we can deal with the threat. Part of the reason why ransomware attacks have been so pervasive is because of the ability to exchange large sums of money without traceability. If we want to definitely eliminate ransomware, governments must regulate cryptocurrencies to shut down the crypto economy. However, that's not realistic – there are legitimate economies running on crypto. Until we eliminate or regulate the cryptocurrency economy, we will keep seeing the rise of ransomware into 2022 and beyond."

CAROLYN CRANDALL, CHIEF SECURITY ADVOCATE, ATTIVO NETWORKS:

"Ransomware will make Active Directory protection a top CISO-level concern. AD is an essential element of an enterprise's network infrastructure, but it is intrinsically insecure and notoriously difficult to protect. Attackers are well aware of its weaknesses and diligently target AD to increase their privileges, escalate their attacks and mass encrypt data for ransom. Active Directory exposures are named as the top reason why ransomware attacks continue to be successful. Business leaders and IT decision makers cannot afford to let visibility and organisational divides leave exposures unaddressed and open for attack.

Moreover, attackers are making it clear that they will not adhere to traditional ethical boundaries. Expect to see more attacks that come dangerous close to or cross the line in impacting human safety. With a new class of attackers coming in, organisations operating in the widely defined role of critical infrastructure – including healthcare, energy and agriculture – will become prime targets in 2022.

Therefore, in 2022 ransomware defences must get a badly needed refresh. Ransomware 3.0 is here, characterised by double extortion where cybercriminals not only encrypt files, but also leak information online that can drastically impact everything from the company's image, profits and stock price. There's no longer a one-size-fits-all approach. One that starts with protecting Active Directory and privileged credentials. In 2022, organisations will be unable to keep up with understanding how each group operates and instead will need to improve their visibility to exposures and add detection measures that are based on technique. Setting up traps, misdirections and speed bump lures along the way will also serve as strong deterrents to keep an attacker from being successful."

> INITIAL ACCESS POINTS LIKE EXPLOITING VULNERABILITIES ARE STILL PERVASIVE ONLINE

KELLY AHUJA, CEO AT VERSA NETWORKS:

"In 2022 it is important to consider MSPs – most of the large-scale Ransomware attacks in the past year have been caused by third-party software being exploited, as evidenced by the SolarWinds and Kaseya hack. More than ever, Managed Service Providers (or MSPs) will be in the best position to be the trusted advisors for all things security to organisations in 2022 and beyond. Critical training on threats and vulnerabilities such as Supply Chain attacks will be a vital component for all Managed Service Providers looking to offer security services and software to their customers. Service Providers and MSPs will have the opportunity to demonstrate that they can effectively and securely manage their customer environments going into 2022. Securing the infrastructure that third-party providers manage requires protection of the people, applications, systems, traffic and everything in-between. MSPs will be trusted advisors who find and retain world-class cybersecurity talent and offer the best training to end users on the modern threats that plague organisations spanning all verticals. Well trained MSP providers acting as trusted advisors to organisations of all sizes will be the foundation for delivering good security hygiene and a strong security strategy for 2022 and beyond."

TODD CARROLL, CISO AT CYBELANGEL:

"In 2022 ransomware will become smaller, but meaner. 2021 was ransomware's coming-out party to the normal world. But with the spotlight came more vigorous enforcement actions being taken against ransomware operators. This will scare away the little fish and ruin a few gangs, but the 'Ransomware as a Service' providers that survive will be hardened like antibiotic-resistant bacteria."

CAN PHISHING LEAD TO RANSOMWARE?

Our newfound dependence on remote and hybrid working catalysed by the Covid-19 pandemic has made targeting employees at home an increasingly fruitful strategy for attackers who recognise that personal mailboxes are often not well protected, and that disbanded workforces are no longer under the watchful eyes of an IT team. Threat artists are exploiting our circumstances in increasingly clever ways in order to launch ransomware attacks and now a new trend is gaining popularity: the fraudulent use of QR codes. See below for details on how hackers are exploiting our increased familiarity with this technology to bypass email gateway defences and deploy their malware to launch a ransomware attack:

> ATTACKERS WILL ALWAYS EXPLOIT EVER-CHANGING CIRCUMSTANCES TO MAXIMISE THEIR PROFIT

MAGNI REYNIR SIGURÐSSON, SENIOR MANAGER OF DETECTION TECHNOLOGIES AT CYREN:

"From track-and-trace to ordering from menus at restaurants, we have seen an increase in QR codes being widely used in multiple industries throughout the past year. The ease of use and accessibility the two-dimensional barcodes have offered customers during the pandemic has meant more and more companies have employed it as part of their business operations. However, threat actors are now exploiting the increased familiarity of this technology by sending out targeted phishing emails containing malicious QR codes.

QR codes are particularly appealing for cybercriminals who look to use them as part of their phishing campaigns, as they negate the need to include URLs or attachments that might get intercepted when scanned by the email gateway, meaning the attackers are much less likely to be detected. QR codes are also 'mobile-friendly' increasing the odds that an unsuspecting victim will follow the malicious URL using a personal or otherwise unsecured device.

These phishing campaigns work on the principle that the victim receives an email, which includes a 'required action' – such as updating or securing an account or paying an outstanding delivery – and therefore subsequently scans the contained QR code. The fraudulent site will then gather any credentials the victim might enter, from usernames and passwords to bank details and social security numbers, and this data will be consequently used by the attackers for malicious purposes.

These types of attacks will only escalate in 2022 as more and more companies start using QR codes for business practice, thereby increasing the surface of legitimate activity for attackers to spoof. Moreover, the new year will see an increase in QR codes being used in malware campaigns, where the fake codes trick users into installing malicious apps via untrusted sites or app-stores that then steal data from the user, such as logging every key stroke, stealing credentials and data, and sending expensive SMS messages from the victim's phone.

The increased use of QR codes and other novel evasion techniques in 2022 will force enhancements to detection technologies and user education. Remember, if the email or text message containing a QR code looks suspicious, it probably is. Consumers can ensure their credentials are safe by enabling multi-factor authentication and following best practices for password management. Businesses should evaluate specialised phishing solutions that employ techniques like machine learning to spot malicious QR codes and other evasive phishing techniques."

LOOKING TOWARDS THE FUTURE:

Ultimately, while it is impossible to perfectly predict the future, with all the success cyber criminals have had throughout the past year they are not going to stop anytime soon. Threat actors will only continue to leverage opportunistic vulnerabilities, so when it comes to protecting your organisation take the advice of the experts and make cyber hygiene your focus in 2022. Proper planning and upkeep will ensure a business can continue to expand their infrastructure and take on new technology without, in the process, becoming the next victim of a devastating ransomware attack ●

Ensuring that all internet-facing infrastructure is security tested should be a priority for all organisations