MUST READ: Have we reached peak ransomware? How the internet's biggest security problem has grown and what happens next

Have we reached peak ransomware? How the internet's biggest security problem has grown and what happens next

A string of high-profile cyberattacks has made ransomware an impossible issue to ignore - in fact, even world leaders are talking about it. Will this be enough to make cyber criminals think twice?

By Danny Palmer | June 22, 2021 -- 11:44 GMT (04:44 PDT) | Topic: Security

Ransomware has become such a significant problem that now even leaders of the global superpowers are discussing these attacks at high-profile summits.

The cyberattacks – which involve criminals encrypting networks and demanding payments that can reach millions of dollars in exchange for the decryption key – were one of the key discussion points during the first face-to-face meeting (https://www.zdnet.com/article/biden-and-putin-spar-over-cybersecurity-ransomware-at-geneva-summit/) of US President Joe Biden and Russian President Vladimir Putin.

Ransomware (https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/) was on the agenda following several high-profile campaigns against US targets, which caused significant disruption.

First, cyber criminals using DarkSide ransomware (https://www.zdnet.com/article/darkside-the-ransomware-group-responsible-for-colonial-pipeline-cyberattack-explained/) hacked the network of Colonial Pipeline (https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/), resulting in services being shut down – disrupting gasoline supplies for much of north eastern United States – and forcing the company to pay a ransom of almost $5 million in bitcoin (https://www.zdnet.com/article/colonial-pipeline-paid-close-to-5-million-in-ransomware-blackmail-payment/). Just weeks later, criminals using REvil ransomware hit meat processor JBS (https://www.zdnet.com/article/fbi-attributes-jbs-ransomware-attack-to-revil/), which paid a ransom of $11 million in bitcoin (https://www.zdnet.com/article/ransomware-meat-firm-jbs-says-it-paid-out-11m-after-attack/).

SEE: Network security policy (https://www.techrepublic.com/resource-library/whitepapers/network-security-policy/?ftag=CMG-01-10aaa1b) **(TechRepublic Premium)**

Like many ransomware groups, both DarkSide and REevil are thought to be the work of cyber criminals working out of Russia. The consensus among cybersecurity researchers is that the Kremlin turns a blind eye to these activities. That's why President Biden directly brought up the issue of ransomware during his meeting with President Putin.

"I looked at him and said: 'How would you feel if ransomware took on the pipelines from your oil fields?' He said: 'It would matter.' I pointed out to him that we have significant cyber capability. And he knows it," Biden told reporters.

Biden's warning to Putin came following the G7 Summit in Cornwall, England, where the leaders of Canada, France, Germany, Italy, Japan, the United Kingdom and the United States issued a joint declaration on ransomware (https://www.zdnet.com/article/ransomware-russia-told-to-tackle-cyber-criminals-operating-from-within-its-borders/), agreeing that international action is needed to combat the issue.

R s been a problem for years, but attacks have become increasingly d amaging for victims while cyber criminals make more and more money

from campaigns. A few years ago, ransoms were hundreds of dollars – now cyber extortionists are demanding millions or even tens of millions of dollars in ransoms.

And ransomware groups are able to keep demanding huge sums of bitcoin and other cryptocurrencies because, for one reason or another, victims are paying the ransoms (https://www.zdnet.com/article/ransomware-too-many-firms-are-still-willing-to-pay-up-if-attacked/).

"It's an effective business model because, from a criminal's point of view, it works because people are paying. Then there are more attacks as a result as it's so successful," says Eleanor Fairford, deputy director for incident management at the National Cyber Security Centre (NCSC).

SEE: Network security policy (https://www.techrepublic.com/resource-library/whitepapers/network-security-policy/) (TechRepublic Premium)

For cyber criminals, ransomware is the easiest and most efficient way to make money from a compromised network.

An intruder within a corporate network could spend months stealing sensitive information then struggle to find a way to make money from it. Or they could use that time and effort to move around a network laying the foundations for a ransomware attack – and walk away with millions of dollars.

The most well-organised ransomware operations will even cherry-pick the organisations they see as potentially the most lucrative or most likely to pay a ransom and focus their efforts on those in order to maximise profits.

"If you're worth $40 million to someone to compromise, is your security good enough to prevent somebody who thinks they can get $40 million out of you? That's a really hard question to answer," says John Hultquist, VP of analysis at Mandiant Threat Intelligence.

"The prices of ransoms has sky-rocketed and it's going to be even harder than ever for organizations to secure themselves against an actor, who can afford advanced capabilities to gain access."

It's because of this situation that hackers are targeting organisations that operate essential infrastructure, factories and other critical services that are reliant on uptime in order to remain functioning. It's possible that an office-based business that gets hit by ransomware c[illegible]e to restore the network without paying a ransom

(https://www.zdnet.com/article/this-company-was-hit-with-ransomware-heres-what-they-did-next-and-why-they-didnt-pay-up/), even if it disrupts services for days or weeks.

Ease of attack

Not only is ransomware a lucrative activity, it's often via relatively simple means that cyber criminals gain access to networks in the first place, exploiting common cybersecurity vulnerabilities (https://www.zdnet.com/article/these-are-the-top-ten-software-flaws-used-by-crooks-make-sure-youve-applied-the-patches/) as the first step in a ransomware attack.

"It's not super-sophisticated zero-day vulnerabilities or that the threat actor wrote an exploit; it's things like VPN without multi-factor authentication, things like unpatched Microsoft Exchange servers (https://www.zdnet.com/article/microsoft-exchange-server-attacks-theyre-being-hacked-faster-than-we-can-count-says-security-company/), it's things like remote desktops on a port that was publicly available to the internet, that are being leveraged for ransomware," says Sherrod DeGrippo, senior director of threat research and detection at Proofpoint.

Despite repeated warnings, organisations may be completely unaware that these vulnerabilities exist or may not have the procedures in place to apply the relevant security patches to close vulnerabilities in RDPs and VPNs (https://www.zdnet.com/article/ransomware-crooks-are-targeting-vulnerable-vpn-devices-in-their-attacks/).

And the COVID-19 pandemic has exacerbated the problem as organisations have far more staff working remotely than before, making it harder to manage security updates or monitor for potentially unusual behaviour (https://www.zdnet.com/article/ransomware-vs-wfh-how-remote-working-is-making-cyberattacks-easier-to-pull-off/).

Ransomware attacks are already damaging and disruptive enough, but many of the most successful ransomware gangs have added another string to their bow – double extortion (https://www.zdnet.com/article/ransomware-theres-been-a-big-rise-in-double-extortion-attacks-as-gangs-try-out-new-tricks/).

SEE: This company was hit by ransomware. Here's what they did next, and why they didn't pay up (https://www.zdnet.com/article/this-company-was-hit-with-ransomware-heres-what-they-did-next-and-why-they-didnt-pay-up/)

Not only do criminals encrypt data and demand a ransom in exchange for a decryption key, th ve gained to the network means they're able to steal sensitive information.

They're not looking to sell it on to rival firms or governments; they simply threaten to publish it if the victim doesn't pay.

It isn't an empty threat, with ransomware gangs running dedicated leak sites where they publish data stolen from organisations that didn't pay up – and that could scare some victims into paying the ransom, although there's no real guarantee that cyber criminals won't exploit that data in the future.

- **'Like playing whack-a-mole': Do cyber-crime crackdowns have any real impact?** (https://www.zdnet.com/article/like-playing-whack-a-mole-do-cyber-crime-crackdowns-have-any-real-impact/)
- **Ransomware attack halts production at IoT maker Sierra Wireless** (https://www.zdnet.com/article/ransomware-attack-halts-production-at-iot-maker-sierra-wireless/)
- **Ransomware gangs have found another set of new targets: Schools and universities** (https://www.zdnet.com/article/ransomware-attacks-against-schools-are-rocketing-with-students-coursework-encrypted/)

Hard-to-trace payments

When organisations do pay the ransom, it's paid in cryptocurrency – and there's an argument that it's helped cyber criminals easily make money from ransomware.

For criminals, getting the money out is the key thing and by using cryptocurrency like bitcoin, they're able to do it in a way that's difficult to trace – and crucially, avoids anything like a regular bank account that could be used to identify them.

"When it comes to cybercrime, monetization becomes really complicated. It's always been sort of the bottleneck – you can get your hands on a bajillion credit-card numbers, but the part where you convert it, that's where everything stops," says Hultquist.

"Cryptocurrencies provided sort of a way around that because it allows them to move this cash freely around outside of regular systems and provided much easier monetization. It's not necessarily the cryptocurrency that is fuelling this, the tremendous payouts are fuelling this. Cryptocurrency just makes the monetization easier," he adds.

The Russian angle

And when ransomware attacks are this financially successful, they'll keep happening – especially if cyber criminals are operating from countries where their governments turn a blind eye to their activities.

The consensus is that many of the most notorious ransomware gangs are operating from within Russia and that they're allowed to make money from ransomware, so long as they focus their activities against the west.

"The Russian state and Russian criminal underworld are not the same thing, but there is understanding between them and understanding is that as far as the state's concerned, Russians can make money a way that suits them," says Ciaran Martin, professor of practice at the University of Oxford's Blavatnik School of Government – and former director of the NCSC.

"But the conditions are: leave Russians and Russian interests alone, and when we need your best people, they have to come; that's the way the model has worked."

SEE: **Ransomware: A company paid millions to get their data back, but forgot to do one thing. So the hackers came back again** (https://www.zdnet.com/article/ransomware-this-is-the-first-thing-you-should-think-about-if-you-fall-victim-to-an-attack/)

Cyber criminals take heed of this warning, with many coding their ransomware with instructions to terminate if a scan reveals that it's on a Russian language system.

On top of this, it's against the Russian constitution to extradite Russian citizens, so even if authorities in the West were able to identify members of a ransomware operation, they're unlikely to be able to make arrests.

Meanwhile, a ransomware group would be unlikely to succeed for long if it was working out of a western nation because law enforcement would quickly take action.

"Why are there no major international ransomware syndicates in the West? Because if you set one up in London or Oxfordshire or Northern Ireland, the National Crime Agency will be kicking down the door within a week, you just couldn't do it," says Martin. "You can't really do it in the West, but you can do in Russia. Why? Because it's allowed."

- **Three billion phishing emails are sent every day. But one change could make life much harder for scammers** (https://www.zdnet.com/article/three-billion-phishing-emails-are-sent-every-day-but-one-change-could-make-life-much-harder-for-scammers/)
- **FBI: Phishing emails are spreading this sophisticated malware** (https://www.zdnet.com/article/fbi-phishing-emails-are-spreading-this-sophisticated-malware/)
- **Largest ransomware demand now stands at $30 million as crooks get bolder** (https://www.zdnet.com/article/largest-ransomware-demand-now-stands-at-30-million-as-crooks-get-bolder/)

Time for change?

Ransomware has been a problem for years – particularly with hospitals regularly falling victim to attacks during the peak of the coronavirus pandemic (https://www.zdnet.com/article/cyber-criminals-targeting-hospitals-are-playing-with-lives-and-must-be-stopped-report-warns/), but the attack against Colonial Pipeline has struck a particular chord.

The pipeline that provides almost half the gasoline supply to the north eastern United States was shut down and that was obvious to all: this wasn't just a business not being able to operate without the use of particular files, this was critical infrastructure that got shut down due to ransomware.

"There will be 'before Colonial Pipeline' and 'after Colonial Pipeline', it's that much of a milestone in the way that the threat actor economy is going to work," says DeGrippo. "It's not a ransom of files any more, it's a ransom of your existence. Ransoming the ability to get hot dogs and beer and gasoline is a whole different ballgame."

The United States has a strong relationship with oil and gas and that made the disruption caused by Colonial Pipeline ransomware attack impossible for the Biden administration to ignore – and it started with the Department of Justice seizing most of the bitcoin used to pay the ransom (https://www.zdnet.com/article/majority-of-ransom-paid-by-colonial-pipeline-seized-and-re

Even the operators of DarkSide ransomware-as-a-service (https://www.zdnet.com/article/ransomware-as-a-service-is-the-new-big-problem-for-business/) attempted to distance themselves from the attack, claiming that "our goal is to make money, and not creating problems for society". They even claim that they'll establish additional checks and balances on their "partners" in future.

But now the ransomware gangs may have bitten off more than they can chew.

"They don't want this much notoriety, they want to be recognised, they want people to pay – but I don't think they necessarily want the US government on their trail – they probably took it a step too far. I'm sure the other ransomware gangs are pretty upset with them," says Hultquist.

The threat from ransomware is still high – as evident by how Ireland's healthcare service continued to suffer disruption weeks on from a Conti ransomware attack (https://www.zdnet.com/article/ransomware-irelands-health-service-is-still-significantly-disrupted-weeks-after-attack/), which hit days after the Colonial Pipeline attack – but there's a feeling that recent events could potentially be a turning point.

"There is at least a plausible case to be made that the past month has been strategically damaging for the criminals and that one hopes that we might – please note, the very careful language – that we might be able to look back at some point on this period as peak ransomware," says Martin.

"Now that's by no means certain yet, it's not even likely yet, but governments are starting to see this can do real harm."

However, in the immediate future, ransomware will remain effective as long as organisations are vulnerable to being hacked by cyber criminals, as demonstrated by how attacks have continued to cause disruption around the world.

But it is possible to build resilience to cyberattacks – including ransomware – and make it much harder for cyber criminals to compromise the network in the first place.

SEE: A winning strategy for cybersecurity (http://www.zdnet.com/topic/a-winning-strategy-for-cybersecurity/) (ZDNet special report) | Download the report as a PDF (https://www.techrepublic.com/resource-library/whitepapers/a-winning-strategy-for-cybersecurity-free-pdf/?ft[illegible]1b) (TechRepublic)

Much of this resilience can be built-up by ensuring that cybersecurity hygiene procedures, such as installing security patches in a timely manner (https://www.zdnet.com/article/this-one-change-could-protect-your-systems-from-attack-so-why-dont-more-companies-do-it/), preventing the use of simple passwords and using multi-factor authentication (https://www.zdnet.com/article/multi-factor-authentication-use-it-for-all-the-people-that-access-your-network-all-the-time/), are applied across the network. Because ransomware gangs are opportunists, by making things more difficult for them, it decreases the likelihood of a successful attack.

"The sorts of things that are useful: having visibility on your network to be able to see if precursor activity is taking place, understanding where your assets and network are, and properly having that mapped and understood. These standard good processes will defend against ransomware," says Fairford.

Regularly updating backups (https://www.zdnet.com/article/a-nas-is-not-enough/) – and storing them offline – also provides another means of lessening the severity of ransomware attacks, because even in the event of the network being encrypted, it's possible to restore it without paying cyber criminals, which cuts off their main means of income.

Nonetheless, the rise of double extortion attacks has added an extra layer of complexity to this issue because if the organisation doesn't pay a ransom, they're faced with the prospect of potentially sensitive information about employees and customers being leaked.

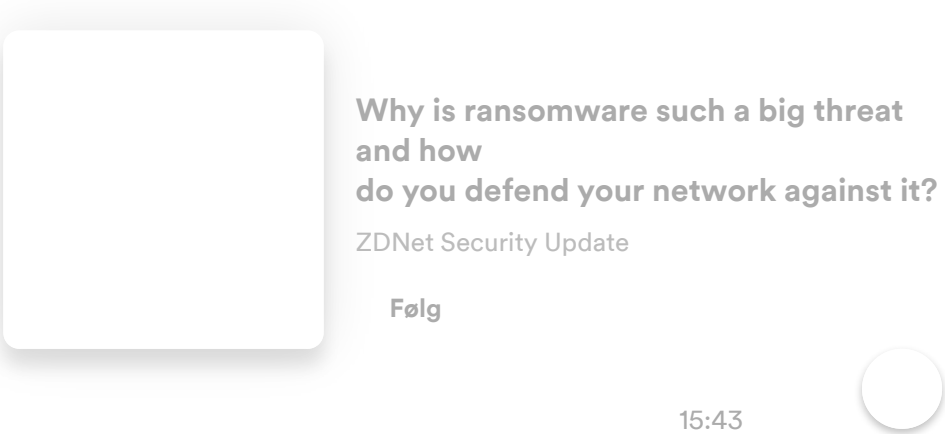
"Do you have a plan if if your information starts leaking out?," says Hultquist. "Those pieces need to be in place now, not when it hits the fan"

The fact that the US and other governments are talking about ransomware should also act as a catalyst for any organisation – that, for whatever reason, didn't have any specific plans for preventing or protecting against a ransomware attack – to decide on their plans now.

Because even in the worst-case scenario, when the network has been encrypted with ransomware, having a set plan can help manage the incident and potentially make it less damaging.

"Companies must sit down with their executives and they must decide, 'if we are a victim of ransomware, how much are we willing to pay, who on the board is going to be authorized to negotiate this and what is our relationship, going to be with law enforcement when it happens?'. Then every quarter, you revisit it and you ask, 'is this still our decision if we c[Cookie Settings]nsomware attack, is this still our plan of action?'" says DeGrippo.

"If you haven't made the decision on how you're going to handle it yet, it's not going to work out in your favour," she adds.



MORE ON CYBERSECURITY

- Ransomware is growing at an alarming rate, warns GCHQ chief (https://www.zdnet.com/article/ransomware-is-growing-at-an-alarming-rate-warns-gchq-chief/)
- White House urges US companies to take ransomware seriously (https://www.techrepublic.com/article/white-house-urges-us-companies-to-take-ransomware-seriously/)
- Ransomware is now a national security risk. This group thinks it knows how to defeat it (https://www.zdnet.com/article/ransomware-is-now-a-national-security-risk-this-group-thinks-it-knows-how-to-defeat-it/)
- New DOJ task force to take on ransomware, says report (https://www.cnet.com/news/new-doj-task-force-to-reportedly-take-on-ransomware/)
- Ransomware: Dramatic increase in attacks is causing harm on a significant scale (https://www.zdnet.com/article/ransomware-dramatic-increase-in-attacks-is-causing-harm-on-a-significant-scale/)

RELATED TOPICS: SECURITY TV | DATA MANAGEMENT | CXO | DATA CENTERS

By Danny Palmer | June 22, 2021 -- 11:44 GMT (04:44 PDT) | Topic: Security

SHOW COMMENTS