beazley

Article

The ransomware regroup

Craig Linton • April 17, 2024

After a temporary decline in ransomware attacks following Russia's February 2022 invasion of Ukraine, hacking groups are reforming and returning to their usual tactics.

The Russian invasion of Ukraine has provoked a far-reaching response from Western countries, most notably in the form of financial sanctions against Russia and military aid to Ukraine. However, predictions that the outbreak of conflict would lead to a dramatic increase in cyber-attacks – whether state-led or by non-state cyber criminals – against NATO members' economies have not come to pass. To understand why this did not happen and why the current lull is not indicative of a new normal, we need to understand the makeup of the cybercrime industry and how it is evolving.

The Ransomware pandemic years

During the ransomware pandemic of 2020-21, Russian cyber criminals, based in Russia or in nearby Russian speaking territories, including Ukraine, were extremely successful in hacking organisations across the globe. These attacks are too numerous to catalogue, but they include the brazen attack on oil infrastructure belonging to Colonial Pipeline and a notable attack on the Washington D.C. Metropolitan Police.1 The circumstances brought about by COVID-19, with organizations globally having to readjust their entire networks to accommodate alternative working arrangements created an environment of reduced security that enabled hackers to find easy targets.

As cybercrime gangs discovered just how vulnerable their victims were and how much they could afford to 'pay up', these gangs turned into a highly professionalised 'industry'. The lucrative proceeds from ransomware attacks attracted new criminals to the industry, with few risks for prosecution at home. Russian and Ukrainian hackers attacked Western businesses with impunity. They could expand in headcount and capability, successfully recruiting hackers to develop their trade and ultimately carry out larger ransomware attacks.

These groups evolved into successful criminal enterprises, employing a

consultancy-style model and training new recruits on easier targets to hone their craft. Larger hacking groups have been found to run physical offices, maintain scheduled working hours, employ managers at various tiers, and use separate departments for HR, coding, training, testing, intelligence gathering, and other functions.2

When the bubble burst

Putin’s invasion of Ukraine burst the cybercrime industry bubble as international hacking groups followed national allegiances and disbanded. Leading groups such as Conti splintered as members joined the war, relocated to flee the conflict, and disbanded over their loyalty to their respective nations.3

The ransomware gang Conti, in particular, had previously attracted attention from the FBI and U.S. State Department, which offered a US$10 million reward for information leading to the identification of key individuals in the group. Elsewhere, some groups responded to the call from the Ukrainian government as it looked to recruit volunteer hackers to help protect its critical infrastructure.4 This ultimately led to a decline in the deployment of ransomware post-invasion, as these groups became less organized and some of their members tilted their focus to the war effort.

The temporary reduction in ransomware attacks was reflected in our Risk & Resilience research data, which shows that the perceived threat of cyber risk to global business leaders peaked in 2021 (34%). According to our Risk & Resilience research, over the past two years concern over cyber risk has declined with just over a quarter (27%) of the business leaders surveyed last year rating cyber risk as their top concern.

The ransomware threat returns

While ransomware activity dipped post-invasion, we are now seeing that the threat for businesses from ransomware groups is intensifying. Russian and Ukrainian hackers are regrouping as the war in Ukraine enters a stalemate. Nationalism is being trumped by the need for money as hackers from both sides of the conflict put aside their differences and reform their networks.

These groups are trying to make up for lost time by demanding heavier ransoms when they successfully hack into firms' data and systems. Previously, hacked firms had settled for ransoms as low as US$200,000 as these groups were less organized and willing to accept smaller fees.5 This compares to ransomware gang BlackCat demanding US$4.5 million after gaining access to Reddit’s internal data in February 2023.6

Furthermore, the threat is intensifying as many industries are now facing a cash crunch in the current tougher market conditions, leading them to invest less in their protection against cyber threats. This is leaving some firms increasingly vulnerable to cybercrime and the resulting damages of a successful attack.

The early signs of a rebound in ransomware activity are visible but the stakes are now higher than ever before. The frequency of larger, more

sophisticated attacks that target organizations of all sizes is on the rise.7 Last year's MOVEit hack – carried out by Russian ransomware gang Clop – resulted in personal data from hundreds of millions of people around the globe being stolen, including members of this author's household.8 It is a timely reminder that businesses remain vulnerable to third-party (and even so-called "fourth-party") cyber-attacks, and need to be vigilant to the threats and risks associated with the knock-on damage that an attack on a software vulnerability of this kind can have.

Layered defense can stem the tide

There are many "in depth" steps that companies can take to help prevent them from becoming a victim of this uptick in ransomware incidents. As we have seen through our underwriting and claims stats policyholders that have better cyber security controls are much less likely to fall victim to a ransomware attack. These steps include actions such as:

- Implementing multi-factor authentication (MFA) for access to network and email resources;
- Protecting and monitoring endpoints through the use of an endpoint protection platform (EPP) and endpoint detection and response (EDR);
- Maintaining asset inventories and installing security patches shortly after notice of a critical vulnerability;
- Reducing the number and usage scope of domain admin accounts;
- Limiting users' permissions and access to role-based need;
- Hardening baseline security configurations of systems, applications, and cloud resources;
- Segmenting networks using strict rules;
- Implementing secure backup solutions that prevent attackers from altering or deleting backups; and
- Having a documented, properly tested, and recently updated incident response and disaster recovery plans

After a period where large hacking groups have been split, it is easy for firms to be lulled into a false sense of security that the decline in ransomware attacks is here to stay. Sadly, the reality is that we are seeing signs that things could start to get ugly once more. I urge businesses of all sizes to take steps to improve their cybersecurity and remain vigilant to the risk of ransomware.

Craig Linton

Head of US Underwriting Management

1- https://www.forbes.com/sites/thomasbrewster/2021/05/13/ransomware-hackers-claim-to-leak-250gb-of-washington-dc-police-data-after-cops-dont-pay-4-million-ransom/

2- https://www.trellix.com/en-au/about/newsroom/stories/research/conti-leaks-examining-the-panama-papers-of-ransomware.html

3- https://www.darkreading.com/attacks-breaches/breakup-conti-ransomware-members-dangerous

4-https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/

5- https://tech.co/news/ransomware-groups-earned-less-last-year

6-https://www.theverge.com/2023/6/19/23765895/reddit-hack-phishing-leak-api-pricing-steve-huffman

7-https://www.beazley.com/en-us/cyber-services-snapshot/defence-depth-cyber-security/latest-trends

8- https://www.bbc.co.uk/news/technology-65814104

beazley