November 23rd, 2021

TLP Amber

This week, *Hacking Healthcare* begins by breaking down the possible ramifications of a new report stating ransomware actors are interested in, and capable of, buying into the zero-day market. We then examine a new Europol report on serious and organized crime that has some interesting things to say about the structure and activities of the European Union (EU) cybercrime ecosystem. Finally, we cover Iran's state-sponsored cyberattacks and detail what might drive even more activity in the near future.

Author's Note: *Yours truly will be at the H-ISAC Summit in San Diego next week. For those of you who will be making the trip, I hope I have the opportunity to meet you.*

1. Ransomware Actors and Zero Days

Ransomware continues to be a lucrative and widespread endeavor, but researchers at Digital Shadows suggest that at least some ransomware actors may not be content with tried and tested methods and are looking for new ways to leverage the fortunes they have gained. In a recently published report, Digital Shadows suggests that there is increasing interest among cybercriminals to enter the zero-day marketplace, and the ramifications could be significant.[1]

This new report suggests that some of the more mature ransomware groups have been so successful that they are now in a financial position to seriously consider purchasing zero-day vulnerabilities and that sellers/developers of such vulnerabilities have moved to engage with them in cybercriminal forums. This would be a concerning development, as the purchase of zero-day vulnerabilities is an activity historically tied only to resource-rich nation-state actors. This exclusivity has largely been a product of the price tag for zero-day vulnerabilities, which can reach into the many millions depending on sophistication and applicability.

You would be right to question why cybercriminals would have any interest in spending millions of dollars on purchasing a zero-day vulnerability when the current process of leveraging longstanding well-known vulnerabilities appears to be working just fine. The rationale appears to be the consideration of an "exploit-as-a-service" model that would "would allow capable threat actors to 'lease' zero-day exploits to other cybercriminals to conduct their attacks."[2] The report notes that zero-day sellers/developers could look to rent out and test zero-days with this approach. This would allow them to confirm the validity of their product while also making money until a definitive buyer could be found.[3]

Action & Analysis

There are reasons to be skeptical that this apparent development will actually mature into something significant in the short term. Outside of a specific target promising an eye-widening payout if it could be compromised, ransomware actors appear to have little incentive to spend the extraordinary amounts of money required to purchase or rent a zero-day vulnerability when so many high-profile and wealthy targets can be compromised by well-known and freely available vulnerabilities. This is especially true when you consider how little progress has been made to stop ransomware, despite its becoming a highly visible priority for years.

It is noteworthy that ransomware groups have been so successful that purchasing zero-day vulnerabilities is even a possibility, but notions that this might lead to ever more sophisticated and unstoppable ransomware attacks are probably overblown. Nation-state actors value zero-days to go after strategic interests where the specificity of a target is key. For ransomware actors, it rarely matters who ends up paying, just so long as someone does.

It will be worth watching if cybercriminal discussions on exploit-as-a-service grows into something tangible, but it's unclear how viable a market there is for something like that. Just because cybercriminals could do something doesn't necessarily mean it's worth their time and effort, and as history has shown, the top cybercriminals are nothing if not ruthlessly efficient and practical. Also, it isn't clear that once the zero-day gets out, cybercriminals would be able to control its distribution effectively enough to make any money. This will be something worth checking on, but healthcare sector entities probably shouldn't rush to add this to their list of things to worry about.

2. Europol: EU Serious and Organized Crime Threat Assessment

Europol, the European Union's (EU) law enforcement agency, recently released its *Serious and Organised Crime Threat Assessment* report. Designed as a "a forward-looking document that assesses shifts in the serious and organised crime landscape," the report covers a wide range of activities, including a breakdown of Europol's perspective on the cybercrime environment.[4] Some of the key takeaways from the report are worth exploring in more depth.

The 108-page report "provides an overview of the current state of knowledge on criminal networks and their operations" and is based on "data provided to Europol by Member States and partners."[5] While much of the report details more traditional criminal enterprises, the sections on cybercrime are fascinating and help to illuminate the structure of EU cybercriminal organizations. Some of the more interesting findings from the report include:[6]

- The number of cybercriminal networks is relatively low, which could be because "cybercrime involves many criminals operating individually and not in the framework of established networks."
- As a result of increased competition and access to online communication tools, violence as a service appears to be increasing and Europol has reason to believe that "violence may become more common to traditionally non-violent criminal activities such as excise fraud or cybercrime."
- "Virtually all criminal activities now feature some online components, such as digital solutions facilitating criminal communications."
- "Law enforcement successes in taking down popular market places, in combination with cyberattacks on platforms, exit fraud or voluntary closures, appear to have generated some distrust among users and may have slowed down the growth of this online environment."
- The belief that critical infrastructure will continue to be targeted in the coming years.
- "Cybercrime is attractive to criminals due to the potential profits, limited risk of detection and prosecution, which if successful often only results in low sentences."
- Europol expects cybercriminal activity related to COVID-19 vaccines to surge, including attacks on pharmaceutical research.
- Worldwide economic trouble may "result in a significant increase in the number of individuals engaging in cybercrime or offering cybercrime-related services."

The freely available report repeats itself occasionally but is straightforward and easily accessible. We encourage those interested in learning more about the findings above, or in the interplay between cybercrime and other crime, to read the full report.

Action & Analysis

Unfortunately, much of the cybercrime section appears to provide a negative outlook for network defenders and law-abiding citizens. One of the key threads that runs throughout the report is how rapidly adaptable the cybercriminal ecosystem is to change. Whether the change is technological, economic, or geopolitical, cybercriminal activity adjusts quickly to take advantage of new vulnerabilities. This evolution appears likely to continually incentivize individuals into the cybercriminal ecosystem as these new vulnerabilities or modes of cybercrime create new opportunities for both new and established actors. Additionally, the recognition that those who engage in these activities rarely face significant punishment, that critical infrastructure will continue to be targeted, and that worldwide economic trouble may further exacerbate individuals turning to cybercrime doesn't bode well.

However, there are reasons to be optimistic. The report does note the increased success of law enforcement actions in taking down cybercriminal infrastructure and the growing distrust among cybercriminals online as competition increases and law enforcement operations become more adept. Additionally, the fact that cyber holds a prominent place in a report like this speaks to the increasing understanding that cybercrime is now a critical component in serious and organized crime, and that it necessitates resources dedicated to it.

3. Rise in Cyber Attacks from Iran

On November 17th, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint advisory with their Australian and UK counterparts, the Australian Cyber Security Centre and the UK's National Cyber Security Centre. The advisory warns that Iranian government-sponsored advanced persistent threat actors (APT) actors are leveraging vulnerabilities in both Microsoft Exchange and Fortinet (a major California-based cybersecurity vendor) in order to gain access to a range of U.S. critical infrastructure organizations in the transport and public health sectors, as well as to some organizations in Australia.[7]

This access enabled various malicious follow-on operations, including data exfiltration, extortion, and ransomware deployment. The malicious activity was observed beginning in March of this year and continuing through the end of October. Notably, in June the

group exploited a Fortinet appliance to access environment control networks associated with a children's hospital in the United States. Additional details on the impact of this specific attack have yet to be published.

A day prior to the federal advisory's publication, Microsoft's Threat Intelligence Center (MSTIC) presented a report at CyberWarCon 2021 on the recent trends in Iranian threat actor activity. In its presentation, MSTIC noted the sophistication and persistence of the Iranian nation-state operators, and their increasing utilization of ransomware to either collect funds or disrupt their targets.

The Microsoft researchers observed at least six different Iranian hacking groups using ransomware to "achieve their strategic objectives."[8] While they did not highlight industry-specific targeting trends, Microsoft researchers noted in a separate report that these Iranian APT groups had been implicated in prior malicious cyber activity, including social engineering attacks during the 2020 U.S. presidential election. The broadening scope of their attacks indicates a desire to both gain access and cause harm to different private industries and government sectors throughout the United States and across different supply chains.

Action & Analysis

Wednesday's federal advisory is one of the first formal and public confirmations of Iranian state-backed hacking. It builds on previous malicious activity by individual Iranian hackers as well as other nation-state hacking organizations, most notoriously, Russia-linked groups.

Increased tensions between Iran and the United States and U.S.-backed allies over numerous issues, including Iran's recent increase of its enriched uranium stockpiles, may make Iranian state-backed cyberattacks more likely. Cyber is one of the few avenues through which Iran can effectively project power and impose costs on its rivals.

The advisory serves as a reminder that not only is the volume of nation-state backed malicious cyber activity increasing, but so too is the number of bad actors involved.[9] It also underscores that ransomware deployment is not limited to just cybercriminals, and that nation-states have recognized "ransomware's potential as a cyberattack capability able to inflict disruptive impacts on victims with low cost and relatively plausible deniability."[10] Given this reality, private companies across all sectors could find value in paying more attention to the international environment and foreign affairs as they build out their cybersecurity and proactively mitigate potential threats.

Finally, on the technical side, the advisory also highlighted the urgent need for all organizations using Microsoft Exchange servers and Fortinet tools to patch their systems

(with a focus on the vulnerabilities CVE-2021-34473, 2018-13379, 2020-12812, and 2019-5591), keep their block lists up to date, employ backup and restoration procedures, regularly back up systems, implement multi-factor authentication, and require strong passwords. We would encourage members to assess implementing these recommendations.

Welcome back to *Hacking Healthcare*.

Congress

Tuesday, November 23rd:
- No relevant hearings

Wednesday, November 24th:
- No relevant hearings

Thursday, November 25th:
- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

Conferences, Webinars, and Summits –

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

[1] https://resources.digitalshadows.com/whitepapers-and-reports/vulnerability-intelligence-do-you-know-where-your-flaws-are?utm_source=blog&utm_medium=website&utm_campaign=vulnerability-report

[2] https://www.digitalshadows.com/blog-and-research/vulnerability-intelligence-whats-the-word-in-dark-web-forums/

[3] https://resources.digitalshadows.com/whitepapers-and-reports/vulnerability-intelligence-do-you-know-where-your-flaws-are?utm_source=blog&utm_medium=website&utm_campaign=vulnerability-report

[4] https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

[5] https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

[6] https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

[7] https://us-cert.cisa.gov/ncas/alerts/aa21-321a

[8] https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/

[9] https://www.meritalk.com/articles/increasing-nation-state-cyber-aggression-prompts-urgent-calls-for-reinforcement/

[10] Cyberwarcon.com/their-own-little-war