Russian cyberattacks pose greater risk to governments and other insights from our annual report

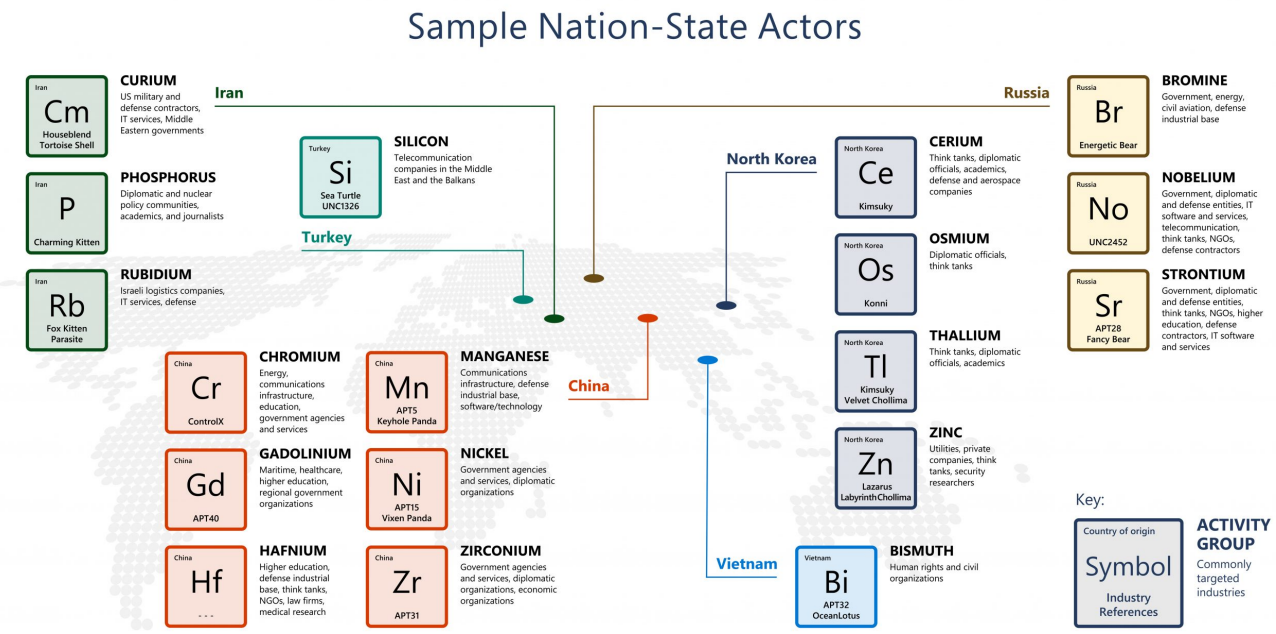
blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/

October 7, 2021

During the past year, 58% of all cyberattacks observed by Microsoft from nation-states have come from Russia. And attacks from Russian nation-state actors are increasingly effective, jumping from a 21% successful compromise rate last year to a 32% rate this year. Russian nation-state actors are increasingly targeting government agencies for intelligence gathering, which jumped from 3% of their targets a year ago to 53% – largely agencies involved in foreign policy, national security or defense. The top three countries targeted by Russian nation-state actors were the United States, Ukraine and the UK.

These are just a few of the insights in the second annual Microsoft Digital Defense Report, which we released today and can be viewed for free here. The Microsoft Digital Defense Report covers the period from July 2020 to June 2021, and its findings cover trends across nation-state activity, cybercrime, supply chain security, hybrid work and disinformation.

Nation-State Activity



Russia is not the only nation-state actor evolving its approaches, and espionage is not the only purpose for nation-state attacks this year.

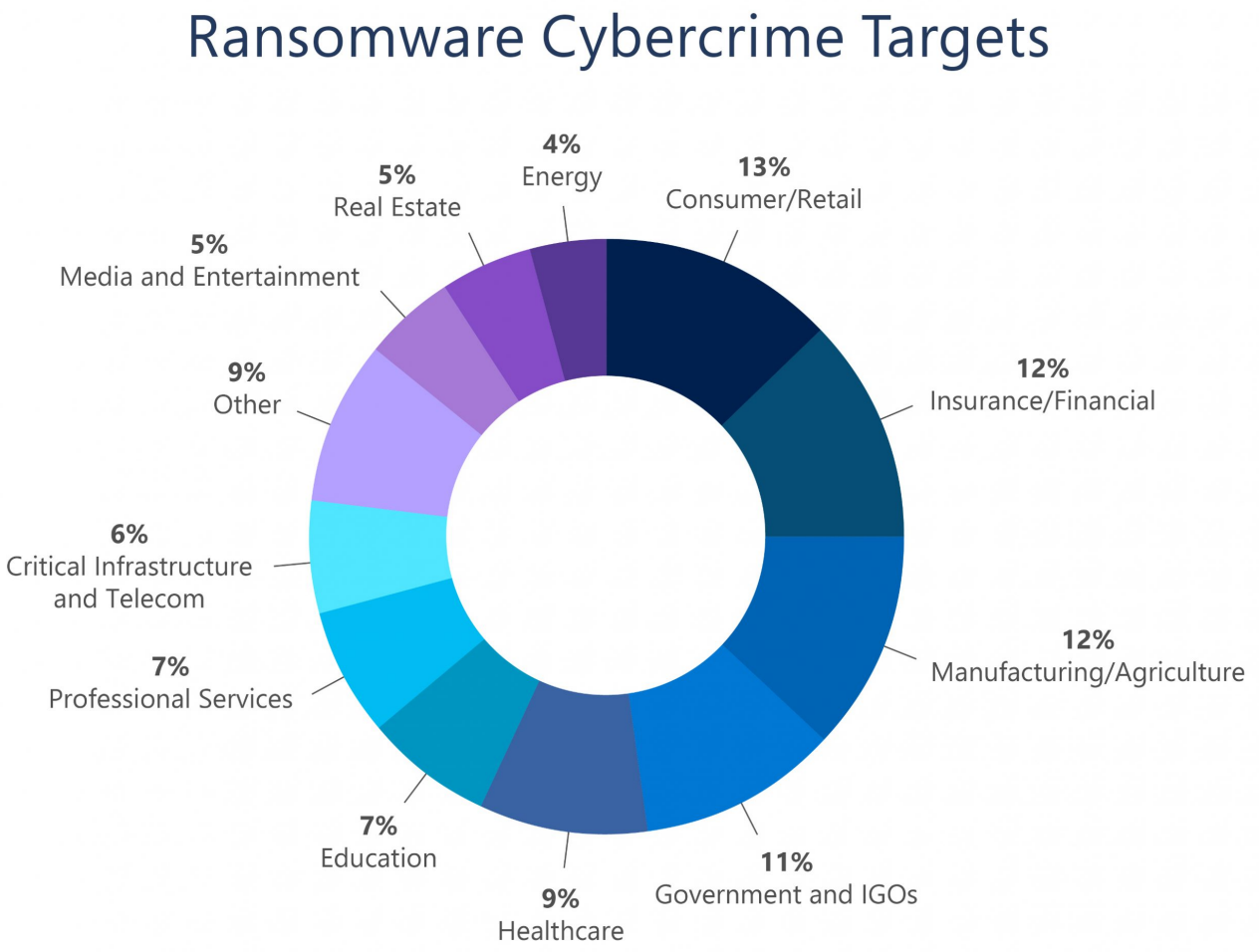
> After Russia, the largest volume of attacks we observed came from North Korea, Iran and China; South Korea, Turkey (a new entrant to our reporting) and Vietnam were also active but represent much less volume.
>
> While espionage is the most common goal for nation-state attacks, some attacker activities reveal other goals, including:
>
> Iran, which quadrupled its targeting of Israel in the past year and launched destructive attacks among heightened tensions between the two countries
>
> North Korea, which targeted cryptocurrency companies for profit as its economy was decimated by sanctions and Covid-19
>
> 21% of attacks we observed across nation-state actors targeted consumers and 79% targeted enterprises with the most targeted sectors being government (48%), NGOs and think tanks (31%), education (3%), intergovernmental organizations (3%), IT (2%), energy (1%) and media (1%).

While China is not unique in its goal of information collection, it has been notable that several Chinese actors have used a range of previously unidentified vulnerabilities. HAFNIUM attacks targeting on-premises Exchange Servers have been well publicized, but, in addition to the zero-day vulnerability used in those attacks, Microsoft detected and reported a Pulse Secure VPN zero day and a SolarWinds zero day earlier this year, both being exploited by Chinese actors.

China is also using its intelligence gathering for a variety of purposes. One Chinese actor, CHROMIUM, has been targeting entities in India, Malaysia, Mongolia, Pakistan and Thailand to glean social, economic and political intelligence about its neighboring countries. Another Chinese actor, NICKEL, has targeted government foreign ministries in Central and South America and Europe. As China's influence shifts with the country's Belt and Road Initiative, we expect these actors will continue to use cyber intelligence gathering for insight into investments, negotiations and influence. Finally, Chinese actors are remarkably persistent; even after we disclosed China's attempts to conduct intelligence collection against individuals involved in the 2020 election, its actor ZIRCONIUM continued its activity during Election Day.

In total, we've notified customers 20,500 times about attempts by all nation-state actors to breach their systems in the past three years. To be clear, Microsoft does not observe every global cyberattack. For example, we have limited visibility into attacks targeting on-premises systems that organizations manage themselves, like the Exchange Server attacks earlier this year, and attacks targeting customers of other technology providers. We believe sharing the data we do have on these threats is helpful to customers, policymakers and the broader security community, and we invite others to share what they're seeing with their visibility. The good news is that our visibility into threats and our ability to help stop them will continue to grow as more organizations move to the cloud.

Cybercrime



Cybercrime – especially ransomware – remains a serious and growing plague as evidenced in this year's Microsoft Digital Defense Report. But while nation-state actors mostly target victims with useful information, cybercriminals target victims with money. As a result, the targets often have a different profile. Cybercrime attacks on critical infrastructure – such as the ransomware attack on Colonial Pipeline – often steal the headlines. However, the top five industries targeted in the past year based on ransomware engagements by our Detection and Response Team (DART) are consumer retail (13%), financial services (12%), manufacturing (12%), government (11%) and health care (9%). The United States is by far the most targeted country, receiving more than triple the ransomware attacks of the next most targeted nation. The U.S. is followed by China, Japan, Germany and the United Arab Emirates.

In the past year, the "cybercrime-as-a-service" economy transitioned from a nascent but rapidly growing industry to a mature criminal enterprise. Today, anyone, regardless of technical knowledge, can access a robust online marketplace to purchase the range of services needed to execute attacks for any purpose. The marketplace has three components. First, as demand has increased, criminals are increasingly focused on specializing in differentiated off-the-shelf infection kits and increasing their use of automation,

driving down their costs and growing their scale. We've seen kits that sell for as little as $66. Second, separate suppliers provide compromised credentials needed to access people's systems and deploy the kits. We've observed credentials selling from $1 to $50 each, depending on the perceived value of the target. Third, cryptocurrency escrow services serve as brokers between buyers and sellers to ensure the kits and credentials perform as offered. We've also begun to identify sophisticated kits that not only provide victim data to the criminal who purchased and deployed the kit but also secretly provide the data to the entity that created the kit.

Ransomware continues to be one of the largest cybercrime threats and, in the past year, it has continued to evolve to become more disruptive. Rather than focus on automated attacks that rely on volume and easily paid low demands to generate profit, human-operated ransomware uses intelligence gleaned from online sources, stealing and studying a victim's financial and insurance documents and investigating compromised networks to select targets and set much higher ransom demands.

Fighting back in a hybrid work environment

As online threats increase in volume, sophistication and impact we must all take steps to strengthen the first line of defense. Deploying fundamental cybersecurity hygiene – like brushing your teeth to protect against cavities or buckling your seatbelt to protect your life – are basic steps we all must take.

Fewer than 20% of our customers are using strong authentication features like multifactor authentication, or MFA. We offer this for free, and organizations can turn it on by default for their users. In fact, if organizations just applied MFA, used anti-malware and kept their systems updated, they would be protected from over 99% of the attacks we see today.

Of course, technology companies like Microsoft have an important role to play in developing secure software, developing advanced cybersecurity products and services for those customers that want to deploy them, and detecting and stopping threats. But organizations taking basic steps to protect themselves will go further than the most sophisticated steps tech companies and governments might take to protect them. The good news is that, in the past 18 months, we've seen a 220% increase in strong authentication usage as companies have thought about increasing their security posture in a remote work environment. The bad news is that we still have a long way to go. Part of the solution needs to be skilling up more cybersecurity professionals who can help organizations of all kinds stay secure, and we'll have more to share on our work in this area in the coming weeks.

There are three trends that also give us hope.

First, the U.S. government has taken unprecedented steps to address cybersecurity using laws and authority already on the books. The Executive Order announced in May has gone a long way to make the U.S. federal government and those it works with more secure, and the

White House's leadership in partnering with the private sector in the midst of the Exchange Server attacks by HAFNIUM earlier this year set a new standard for incident-related collaboration.

Second, governments around the world are introducing and passing new laws requiring things like mandatory reporting when organizations discover cyberattacks so that appropriate government agencies have a sense for scope of the problem and can investigate incidents using their resources.

Third, both governments and companies are voluntarily coming forward when they're the victims of attacks. This transparency helps everyone better understand the problem and enables increased engagement from government and first responders.

The trends are clear: nation-states are increasingly using, and will continue to use, cyberattacks for whatever their political objectives are, whether those are espionage, disruption or destruction. We anticipate more countries will join the list of those engaging in offensive cyber operations, and that those operations will become more brazen, persistent and damaging unless there are more serious consequences. And the cybercrime market will continue to become more sophisticated and more specialized unless we all evolve our work to stop them. More work than ever is underway to counteract these concerns, but we will need to ensure they remain on the top of national and international agendas in the coming years.

Tags: cyber, cybersecurity, Microsoft Digital Defense Report, ransomware