Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Critical infrastructure under attack: lessons from a honeypot

Israel Barak, Cybereason

As its name suggests, critical infrastructure is just that – critical. It includes facilities, information, processes and systems upon which our society functions and depends – from energy and our water supply, to transport, election systems and the government. The health sector too is pivotal in supporting everyday citizens and never has this been clearer than today, in the midst of a pandemic.

Indeed, due to Covid-19, one could argue that the remit of critical infrastructure may have even expanded beyond our ‘traditional’ understanding. For instance, it is no longer enough to classify the ‘food production supply chain’ under critical infrastructure without also including the retailers, or grocery stores, that bridge the gap between supplier and consumer. Either way, the vital nature of these various services and goods puts a target on their back, from both organised cyber-crime gangs and state-sponsored actors.

In targeting these institutions, the stakes are decidedly heightened as well. Formerly, a cyber attack may have resulted in the loss or exposure of data, perhaps financial information – no doubt a grievous offence. Nevertheless, an attack on critical infrastructure, physically puts individuals at risk of harm, perhaps even death. In an almost dystopic, ‘Black Mirror’ example, the hijacking of a food-processing plant may result in false readings of hygiene levels, allergens, toxic elements etc, the consequences of which would be dire. Yet, choosing to believe that such catastrophic incidents are confined to the television screen would be a grave mistake, and one that serves up our safety and well-being on a silver platter.

Just a few months ago, in April 2020, the Portuguese energy giant, EDP, suffered a ransomware attack that saw 10TB of sensitive corporate data stolen and used to blackmail the corporation for nearly $11m.1 In June 2020, Australian Prime Minister Scott Morrison informed the public of a string of malicious attacks being executed against the government, industry, education and other essential service providers.2 And earlier this month, explosions at an Iranian nuclear facility were reportedly the result of an Israeli cyber attack – an alleged act of retaliation following the Iranian cyber attack on Israeli water systems two months prior.3 Knowing this, critical infrastructure operators have every reason to be on high alert and to improve their defences. A part of being able to do so is through understanding the strategy of these bad actors. So, what is it?

Earlier this year, Cybereason launched its second ICS network honeypot to learn tactics, techniques and procedures (TTPs) of the criminal underworld as attacks against these environments continue to increase.

Setting the trap

Much like flies are drawn to a pool of honey, a honeypot is a computer system that simulates a target that lures in hackers. In this case, Cybereason constructed a network architecture that mimicked an electrical company operating in North America and Europe. It included an IT environment, an operational technology (OT) environment as well as human machine interface (HMI) management systems, a dashboard that allows a person to control corresponding devices. Moreover, embedded within the setup were security vulnerabilities typically found in such environments, as well as similar controls such as network segmentation. From there, a team watched as attackers began to bite.

Only three days after the honeypot went live, hackers began to exploit it with a variety of ransomware attacks. In order to infiltrate the system, they began by targeting publicly accessible remote administration interfaces. It is through these interfaces that network operators provide technicians with access to the network and troubleshoot any issues or carry out maintenance work. In other words, the interface offers individuals the ability to perform privileged actions, making it a valuable mark for these hackers. Eventually, they were able to log in through brute force, using information gathered in real time from the honeypot environment.

Once through, the hackers exploited the use of fileless malware. While in the past malware was typically installed through a file or software, a fileless attack takes advantage of existing, legitimate tools to accomplish malicious plans, making it much harder to detect. In this case, a PowerShell script, or command codes, were utilised to open a backdoor for an ‘admin’ user. In doing so, these users were able to continue their efforts without raising any red flags.

From there, further attack tools were uploaded with the help of PowerShell. This included Mimikatz, an open-source application used to steal credentials. Through employing this new tool and the use of the PSEexec remote execution utility, the attackers attempted to garner authorisations to other user accounts and move laterally across the network.
towards the domain controllers. In this instance, the bad actors failed to gain access to domain controllers as none of the accounts within the honeypot environment had these permissions. Nevertheless, they persisted in moving laterally, using network scanners to identify other possible endpoints. It was only when every endpoint had been penetrated that the attacker then dispensed the ransomware.

Interestingly, much like a python coiling around its prey, there appears to be a rising trend for attackers to become deeply embedded within a system before detonating their ransomware – making sure to not attack at the earliest opportunity but to first affect as many machines as possible, while amassing credentials. In doing so, they are guaranteed a bigger payday. This strategy differs from what we witnessed in a near identical honey-pot conducted back in 2018.

Cyber attacks evolve

In the beginning stages of the 2018 experiment, the hackers appeared to operate in a similar manner to the most recent honeypot. That is, exploiting remote access services and installing a backdoor, which allows bad actors to gain access to the network, regardless of whether there is a change in administrator passwords. In this case, however, the tool, xDedic RDP Patch, was also installed, suggesting that a black market seller had discovered the environment and was intending to sell it on xDedic.

Yet, unlike the 2020 honeypot which operated in a stealthier fashion, the hacker who first identified the environment almost immediately began unleashing a flood of attacks. This included crypto-mining bots, phishing bots and distributed denial of service (DDoS) bots. It was only 10 days later, when a new owner had connected to the environment, that work was done to move laterally across the network – more specifically, to identify a path from the IT to the OT environment. The attacker was also less concerned with scanning the full network for all endpoints and more interested in pinpointing an entryway into the HMI and OT controllers.

What’s more, it appears that ransomware attacks have pivoted slightly. In 2018, the ransomware employed typically included file encryption capabilities. Yet, in 2020, on top of file encryption, the attackers had also added the ability to run hacking operations. In this way, present-day ransomware is more effective at milking each attack for what it is worth.

Once bitten, twice shy

There is no doubt that cyber criminals have become more sophisticated in their attacks, now choosing to adopt a more-targeted, multi-stage approach to reap greater financial rewards. They are no longer content with holding a network for ransom but exploiting every single vulnerability within it. If we hope to avoid a nationwide blackout or worse, security teams will need to adhere to three best practices.

First and foremost, critical infrastructure operators should aim to minimise mean time to response. In other words, organisations should establish the response tools and procedures in both IT as well as OT networks to respond to a threat as quickly as possible. One way of doing this is through implementing a threat-hunting service that runs on a 24/7 basis.

Second, it is critical to have visibility – more specifically, visibility between the IT and OT environments as attackers are keen to gain access to the OT environment where their actions can produce more damaging, physical results. In order to do so, organisations should build a security operations centre (SOC). This team of security analysts and engineers can help in overseeing the cyber security operations of the entire organisation and assist in offering a more comprehensive, cohesive and efficient response to threats.

Last but not least, security needs to be in the fabric, or DNA, of any critical infrastructure system. That is to say, built from the design stage and into its operation. Security teams need to be prepared, knowing what threats currently exist as well as how they are evolving.

To be certain that all bases are covered, organisations would do well to partner with experts in ICS threats. Indeed, the public and private sector should team up against the common enemy. Running drills, or table-top exercises between red and blue teams, would also be highly beneficial as it allows security teams to consider every possible scenario, patch any vulnerabilities and create a roadmap in the unfortunate event of an attack.

About the author

Israel Barak is a cyber defence and warfare expert, with an extensive background in working for government organisations, where he established and operated various cyber warfare teams. As Cybereason’s CISO, he is at the forefront of the company’s security innovation, as well as research and analysis of current and evolving advanced threats. As part of his various roles, Barak has developed cyber warfare infrastructure and proprietary technologies, including leading development of proprietary cryptographic solutions, research and analysis of security vulnerabilities, information security products and technologies, and managed enterprise-wide large scale development and implementation projects of cyber technologies. He spent years training, guiding and professionally mentoring new personnel, providing in-depth cyber expertise as it relates to cyber warfare, cyber security and threat actors’ tactics and procedures. He is a regular speaker at leading cyber security industry conferences and events.

References

1. ‘Energy Giant EDP suffers ransomware attack; hackers demand $10.9m’. Teiss, 20 Apr 2020. Accessed Sep 2020. www.teiss.co.uk/cyber-attack-report.
2. ‘Australia cyber attacks: PM Morrison warns of ‘sophisticated’ state hack’. BBC News, 19 Jun 2020. Accessed Sep 2020. www.bbc.com/news/world-australia-46096768.
3. Kundaliya, Dev. ‘Explosion at Iran’s nuclear facility caused by Israeli cyber attack, report’. Computing, 6 Jul 2020. Accessed Sep 2020. www.computing.co.uk/news/4017379/explosion-iran-nuclear-facility-caused-israeli-cyber-attack-report.