Jul 22, 2021 16:25 CEST

Fighting the ransomware war

By LogPoint CTO Christian Have

Ransomware attacks are becoming increasingly devastating to companies. Not only do they inflict massive disruptions to operations, but criminals are also asking for ever-larger ransoms to unlock the encrypted files and machines hit by the attacks.

Throughout the last months, state-sponsored ransomware attacks inflicting damage on critical infrastructure have dominated the headlines. JBS recently paid 11 million dollars following an attack that shut down all the companies' U.S. beef plants. Just before that, an attack paralyzed Ireland's health services for weeks in the middle of a pandemic. The attack happened in the wake of the Colonial Pipeline attack that caused fear of gas shortages.

CNA Financial, one of the largest insurance companies in the U.S., reportedly paid 40 million dollars to get access to its files and to restore its operations, making it the largest reported ransom paid to date. In comparison, 40 million dollars is more than most companies spend on their cybersecurity budget – it is even more than what many companies spend on their entire IT budget.

Due to the surges in state-sponsored ransomware attacks in the U.S. and Europe, many government institutions, including the White House, have urged companies to bolster their defenses to help stop the ransomware groups. The G7 group has called on Russia, in particular, to identify, disrupt, and hold to account those within its borders who conduct ransomware attacks and other cybercrimes. One of the few outcomes of the Biden-Putin summit is an agreement to consult on cybersecurity. However, the agreement is ambiguous without any specific actions.

The ransomware ecosystem explained – a ransom payout isn't always the end goal

Stopping ransomware groups is no small task. The scale of the economy behind these groups is significant. Many active groups have corporate structures, with roles and responsibilities that mirror regular software development organizations.

The indictment of TrickBot's members, who had defined roles in managing the malware. Source: Twitter.

These criminal organizations are well-funded and highly motivated to develop their attacks – but their revenue streams do not begin or end with victims paying up a ransom. There is an entire ransomware ecosystem, capitalizing on successfully executing attacks, such as:

- Groups selling access to platforms that deliver end-to-end ransomware-as-a-service for other groups to use.
- Brokers that deliver teams of highly specialized developers that can build and deploy malware. Think of this as malware recruiting.
- Certain groups only gain access to corporate networks. They will not actively disrupt the operations or demand ransom; instead, they sell access to victims for other groups to capitalize on.

The increasing sophistication of ransomware groups has led many organizations to implement a multitude of tools to help detect and prevent attacks. But what really works?

Basic security is essential to prevent ransomware attacks

For the last 15 years, CISOs, security operations teams and security vendors have put a significant focus on complex attacks and staying on top of the cutting edge of what adversaries can do. For example, the malicious computer worm Stuxnet launches extremely advanced campaigns. The result is that a lot of organizations have a relatively extensive portfolio of advanced technologies. These technologies are expensive, complex to use and even more complex to integrate with each other and the surrounding security ecosystem.

The Colonial Pipeline breach happened because a remote access platform failed to enforce or require multi-factor authentication. Combined with a shared password used among several users, attackers found a way into the infrastructure. Advanced detection tools are not meant to detect such basic mistakes.

Failing to cover the basics – patching, secure configurations or following best practices – is a pattern repeating itself in many of the recent attacks. It is not without reason that every authority on cybersecurity has patching and baselining configurations as some of the first recommendations for companies to strengthen their cybersecurity efforts.

So why are companies not just patching everything, implementing the Zero Trust model and forcing multi-factor authentication everywhere? Especially when the most considerable material risk to the operations and existence of the organization is a ransomware attack?

IT operations is hard. The security operations team, IT operations team and enterprise risk management team often have siloed thinking with different objectives and incentives. Aligning activities and goals across various departments is, without a doubt, part of the problem.

One of the things we hear from our customers is that they need a unified overview of the technical risk aspects. Implementing a unified solution such as ZeroTrust orchestration or XDR is complex and, in many cases, expensive. Some of our customers are turning to fewer vendors and relying on open standards for example MITRE for a taxonomy of attacks, MISP to share threat observations and YARA to identify malware indicators to offload some of the headaches of aligning different departments' ways of working.

LogPoint working to strengthen ransomware defense

LogPoint can help organizations align detection and response activities. LogPoint ingests log data, which security teams can use to easily detect ransomware variants like FiveHands, Egregor, or Ryuk. The REvil group that hit JBS uses a tactic to delete Shadow Copies before encryption. Deleting Shadow Copies makes a restore significantly more difficult. LogPoint can immediately detect deletion of Shadow Copies by looking for the following command across all log sources:

Ingesting log data allows analysts to interrogate systems for more information about known issues, such as detected vulnerabilities, deviations from best practices or enterprise policies. However, combining log data with vulnerability data, configuration compliance and more advanced interrogation of the system, we can uncover the unknown issues by formulating more exact risk scores of the infrastructure and its components.

With the risk scores nailed down, we are currently working on coupling indicators of ransomware, such as the deletion of Shadow Copies, with threat intelligence and malware research to identify documented adversarial techniques. The goal is that the system can conclude the type of ransomware group or variant, so we are more prepared to deal with and respond to the threat. Our system uses a combination of natural language processing and machine learning to connect the dots.

We are also working with our customers on building the final step – automating and orchestrating the response with situational awareness and understanding of the next phase of the attack. We have small agents deployed on our customers' machines that can enforce policies, disconnect machines from networks and otherwise act based on how security operators want to approach a potential issue.

Steps to end the vicious ransomware cycle

At the end of the day, it becomes clear to security researchers who are following ransomware groups that the asymmetry between the capabilities and the incentive for the attackers and the maturity and budgets of the defenders is becoming more pronounced. When critical infrastructure is under attack through large and small companies, it is obvious that more technology will not solve the issue alone. Outsourcing IT operations or security operations alone is not solving the problem either.

With that in mind, I see three paths forward:

- Law enforcement agencies must cooperate across borders to target ransomware groups, track payments and ultimately change the operational risk for these groups so that it is more expensive to do illicit business.
- Breaking down silos within organizations, getting the cybersecurity, IT operations and risk management teams to speak the same language and align expectations. Who owns the backup – IT? Who is responsible for the disaster recovery – Security? Who owns the business continuity planning – Enterprise risk management?
- More laws and regulations on the matter. GDPR has done a lot to bring focus and awareness about reporting breaches to infrastructure. But more is needed. GPDR works for personal data, but disruptions to critical infrastructure following a ransomware attack are not necessarily under the umbrella of GDPR and, as such, can go under the radar. With more sharing, increased focus and potentially fines levied against organizations that fail to prevent or protect their infrastructure adequately, boardrooms will begin to take the threat seriously.

About Logpoint
Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats. By combining sophisticated technology and a profound understanding of customer challenges, LogPoint bolsters security teams' capabilities while helping them combat current and future threats. Logpoint offers SIEM, UEBA, SOAR and BCS technologies converged into a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more. Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company. For more information, visit http://www.logpoint.com

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98