LogicHub

5 Things that SOCs Should Know About Ransomware

Ransomware – malware that encrypts data and locks down machines until a ransom is paid, usually by means of a digital currency – has been a serious and growing problem for years. It has crippled the computers of millions of consumers. It has temporarily shut down the National Health Service in the UK in 2017, causing the cancellation of 19,000 appointments and ringing up a £92m tab. It stopped the daily operations of Atlanta's city government for a solid week, leading to recovery costs of $17m. And in aggregate it's estimated to cost businesses about $75 billion per year.

Security professionals know that ransomware is a major problem. But attack patterns are changing, and the defense strategy that worked in 2018 is less likely to be successful now.

Here are five things that every SOC should know about detecting and stopping ransomware attacks.

1. Attackers are shifting their attention from consumers to businesses and governments.

Ransomware attacks grew in 2016 and 2017, then declined in 2018, and are on the rise again. But ransomware variants are changing and so are their targets. The GandCrab ransomware-as-a-service variant, which was used widely to attack consumers over 15 months, has seemingly shut down after generating $2 billion in ransom payments and earning its creators (according to their own account anyway) $150 million in profits.

Meanwhile, the high payouts attackers have received from healthcare organizations and governments recently seems to have prompted a shift in strategy. Businesses and governments seem to be a new focus in attacks. When attackers threaten to stop hospitals from treating patients or city governments from serving their citizens, crime can pay.

2. Attackers seem to be conducting open source intelligence gathering (OSINT) so they can focus on vulnerable, high-stakes systems.

To hit systems that organizations can't live without their data and internet connectivity without being detected early on, attackers seem to be conducting OSINT research to discover which systems are

vulnerable, which users should be phished, and so on. What this means for SOCs is that the stakes for detection are high; an attack is liable to be pinpointed, well researched, stealthy, and costly.

3. Insurance companies have begun encouraging their clients to pay ransoms, which validates the ransomware business model and may lead to more businesses and governments being attacked.

You can almost understand an insurance company's point of view. An insurance company's charter is to minimize the damage and expenses accrued by clients, and they have a client whose operations have been crippled by ransomware. Ransomware itself doesn't seem to be going away. So clients should just pay the ransom and get on with their lives, stopping losses and returning to generating profits, even if that client's payment just further reinforces the idea that ransomware works.

Or an insurance client might do the math and decide to pay without any urging at all from their insurance company. Attackers were demanding $470,000 to restore the data belonging to the government offices in Lake City, Florida. The city decided to pay, reasoning that its insurance company would cover most of the costs. The city itself ended up paying only the deductible, a mere $10,000. And files and internet service were restored.

Attackers, of course, can see the pattern here. They may have more confidence that an attack will be lucrative if they target a company in finance, healthcare, energy, transportation, or other markets with high-stakes operations. In other words, if they target companies that need to keep operating 24/7 and may have purchased cyber insurance to ensure they can do so in the event of an attack.

SOCs in companies in these markets should prepare to be targeted by hackers.

4. Phishing remains a popular vector for attack, so automating phishing triage is an important part of defending against ransomware and other email-borne attacks.

Techniques for spreading ransomware vary, but phishing remains a popular means of distributing ransomware. SOCs have lots of reasons for stopping phishing attacks—avoiding data breaches among them. But coming up with a way to block or triage phishing attacks quickly is an important part of preventing ransomware infections from starting or spreading across the organization.

It's also prudent to educate employees about phishing, malvertising, and other likely attack vectors.

5. Ransomware attacks are becoming more subtle, requiring new techniques for detection.

New ransomware variants are designed to elude detection by automatically sensing sandboxes (quarantined environments for testing software to see if it is malicious) or using file-less attacks that "live off the land" by using PowerShell or other Windows Process Creation events. Along with defending against phishing, SOCs should make sure they can detect these other subtle attack vectors so they can stop ransomware from infecting the organization.

The LogicHub SOAR+ Security Automation Platform and Ransomware

The LogicHub SOAR+ security automation platform provides SOCs with a powerful solution for automation threat detection, threat hunting, and alert triage. LogicHub is the only solution to automate decisions about threat hunting, threat detection, alert triage and incident response in a single platform.

The platform autonomously guides security operations personnel through difficult and time-consuming decision-making processes. It does so by building detailed contextual models for advanced threat analysis and virtualizing the expertise of level-3 security analysts to deliver expert recommendations in real-time.

The platform offers automated features that are critical for detecting and stopping ransomware. These features include:

- Autonomous playbooks for detecting and stopping file-less, "living off the land" attacks
- Autonomous playbooks for detecting and stopping phishing attacks
- Automated alert triage that frees security analysts to engage in more proactive threat hunting and threat detection

To learn more about how the LogicHub platform can help your organization defend against ransomware and other security attacks, please contact us.

LogicHub

a: 301 N Whisman Rd Mountain View, CA 94043
w: www.logichub.com
e: info@logichub.com
p: (650) 262-3756