Ransomware of Things: When Ransomware and IoT Collide

Companies Unprepared for Next Big Cybersecurity Threat

Arctic Wolf conducted a survey of mid-market companies and found that most still had rudimentary cybersecurity. Despite high profile ransomware attacks such as WannaCry and Petya, small enterprises largely do not have advanced detection and response capabilities for ransomware, advanced persistent threats (APT) and zero day attacks.

SMB Security is rudimentary:

- 80% do not have products to protect against zero day threats
- 62% do not do log analysis

Ransomware response plans lacking:

- 69% do not have formal incident response plan
- 45% would pay the ransom

IoT cyberattacks are a reality

- 100% use at least one IoT device
- 29% transportation companies experienced IoT attack

The survey also found that these companies have embraced the Internet of Things (IoT). The adoption of IoT is due to the productivity and convenience Internet-enabled devices can provide to a business. But the combination of rudimentary security and rapid IoT adoption makes mid-market companies prime targets for the next big cybersecurity threat: the ransomware of things.

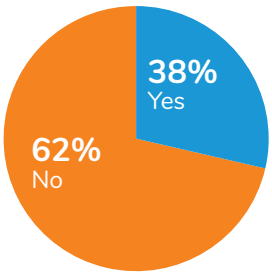
Cybersecurity is Rudimentary

Nearly every company has a firewall and antivirus in place, and many also go a step further and do web content filtering. With today's threat landscape, these are just the basics. Unfortunately most companies seem to have stopped here, which leaves them vulnerable to ransomware and APTs. These advanced threats can easily bypass these basic security measures and often do.

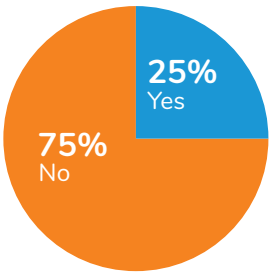
Log collection and analysis and the use of third party threat intelligence provide a more comprehensive layer of security that can protect against today's advanced cyberattacks and ransomware. Such comprehensive security methods require skilled security engineers and a SIEM, and companies doing this usually have a team of four to eight people to do this. Mid-market companies with lean IT teams usually do not have the budget or expertise so rely on traditional perimeter and endpoint products for their cybersecurity.

Only 38 percent of survey respondents answered they used log analysis tools and products, and only 25 percent indicated they used external threat data. Companies that do not analyze their log data or leverage third party threat intelligence are operating with severe security blind spots that can lead to undetected security breaches, and may even be able to prevent known security threats.

Percent of Companies that Perform Log Analysis



Percent of Companies Using Third Party Threat Data

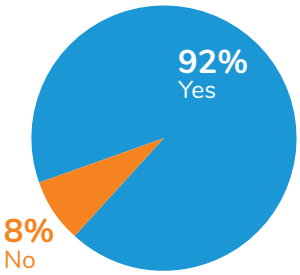


Ransomware and IoT Security Top of Mind

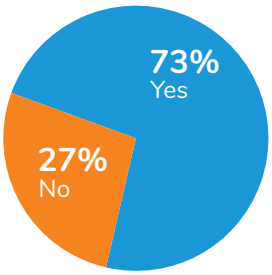
2016 was the year of ransomware, and it has carried over into 2017. The FBI estimates that ransomware is a billion dollar business for cybercriminals. Ransomware has become so lucrative, cybercriminals are now offering ransomware-as-a-service, making it easy for criminals to get started with zero to minimal up-front costs.

The survey found that mid-market companies are almost equally concerned about IoT security as they are about ransomware. 92 percent of survey respondents indicated they were concerned about ransomware, and 73 percent indicated they were also concerned about IoT security.

Concerned About Ransomware

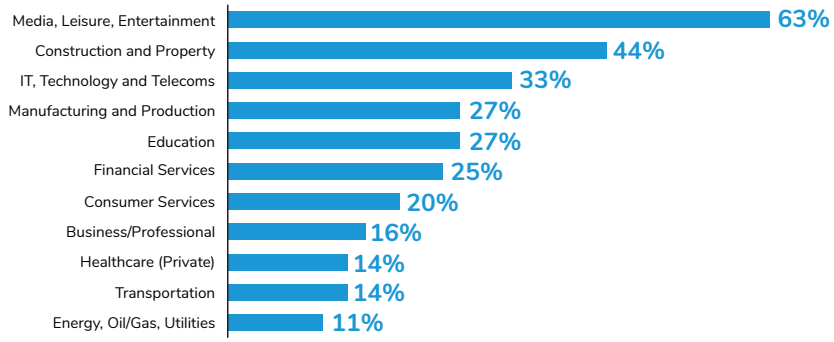


At Risk for IoT Security Breach



Mid-market companies are overwhelmingly concerned about ransomware. Respondents from the industry experienced a 63 percent rate of attack from ransomware. What is clear from the survey results is that no company is immune. Size also does not seem to be a factor, with 22 percent of companies with 200-499 employees indicating they had been attacked by ransomware.

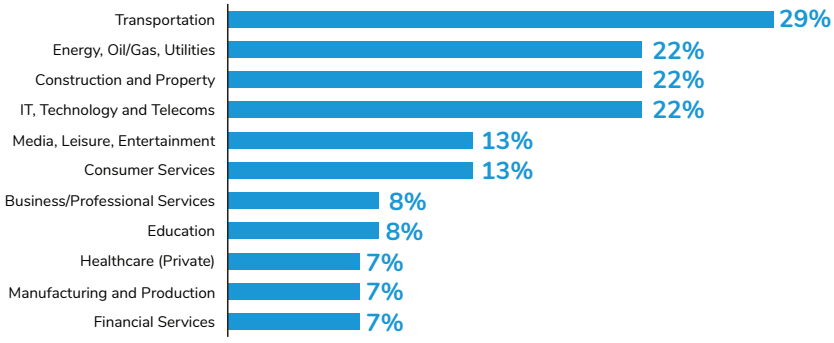
Incidence of Ransomware Attack by Industry



Incidence of Ransomware Attack by Size

With the adoption of IoT, cyberattacks on IoT devices appear to be emerging and becoming more commonplace. 29 percent of transportation companies indicated they experienced an IoT attack, which implies that cybercriminals are already focusing their efforts on IoT-based cyberattacks. Companies in the energy, construction and technology industries also seem to be targeted for IoT attacks.

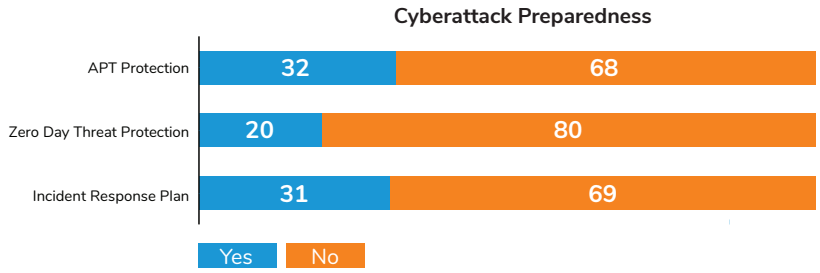
Incidence of IoT-Based Attack by Industry



Incidence of IoT-Based Attack by Size

Unprepared for Ransomware of Things

The rudimentary security measures of mid-market companies also comes through with their lack of protective measures against APT and zero day threats. 68 percent of survey respondents did not use products to protect themselves against APTs, and 80 percent of respondents did not use products to protect against zero day threats. 69 percent of respondents also indicated they do not have a formal incident response plan in place.



The combination of these three data points indicate that mid-market companies are not prepared for today's threat landscape, where ransomware is constantly evolving to infiltrate a company's defenses in new ways. Kaspersky Lab, an antivirus company, reported that in one quarter in 2016, more than 32,000 new ransomware variations were reported. This shows that cybercriminals are constantly innovating and highlights why ransomware attacks continue to be successful.

With ransomware still on the rise and IoT technology becoming more prevalent, cyber-criminals will inevitably create turn to ransomware of things and begin extorting ransoms in new ways. Cyberattacks on water and electric systems have already been reported. White hat hackers have also demonstrated how cars can be hijacked remotely. The question is not if, but when ransomware of things attacks become more prevalent.

Security Operations Center Improves Cybersecurity

A security operations center (SOC) is the most essential element of modern security, but they are often viewed as very expensive and complicated. The Arctic Wolf "The State of Mid-Market Cybersecurity: 2017" survey found that a SOC was highly desired by survey respondents, but largely viewed as being outside of their budget. 88 percent of respondents believed that a SOC would be beneficial for their business, while 59 percent reported that a SOC was too expensive. The data showed that a SOC on average costs $1.4 million to establish, and the ongoing operational costs are also significant.

Would having a SOC improve your organization's security?

About the Survey

The survey data came from the responses of 300 respondents who were responsible for the IT or security function in their company. The respondents worked at companies with between 200 to 3,000 employees. 93 percent of the respondents were director level or higher with budgetary authority or direct organizational authority for security

About Arctic Wolf

Arctic Wolf Networks provides SOC-as-a-service that is redefining the economics of security. AWN CyberSOC is anchored by Concierge Security Engineers and includes 24x7 monitoring, custom alerting and incident investigation and response. There is no hardware or software to purchase, and the end-to-end service includes a proprietary cloud-based SIEM, threat intelligence subscriptions and all the expertise and tools required.

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com