To Pay or Not to Pay: Ransom-Based Cyber-Attacks on the Rise

Like a flu bug that morphs and mutates only to come back stronger, ransomware is here to stay. Unfortunately, there is no vaccine to stop this type of malware and much of its staying power can be attributed to the creativity of its authors.

Over the past decade, ransomware has spread to all corners of the globe, successfully targeting hundreds of thousands of business systems and home PCs. The losses are mounting: the FBI reported a loss of $18 million[1] over a 15-month period in 2014 and 2015 due to ransomware attacks.

Ransom-based attacks are on the rise, and businesses face a growing threat from these financially-driven cyber assaulters. In general, these attacks come in two primary "flavors."

- **Ransomware** – attackers typically use malware to encrypt critical data, making it unusable until the user complies with instructions to make a payment, usually via Bitcoin. One of the latest varieties to emerge is Ransom32, which is ransomware as-a-service that gives cyber criminals a jumpstart on holding victims' information hostage.

- **DDoS for ransom** – attackers send their target a letter that threatens a DDoS attack at a certain day and time unless the organization makes a payment (usually $2,000 to $10,000) via Bitcoin. Often hackers will launch a small-scale attack as a preview of what could follow.

Research from Radware has shown that organizations can expect an increase in these financially-motivated cyber assaults. Ransom-oriented attacks accounted for about one-quarter of motivations in 2015 (versus 16% in the prior year), according to the *2015-2016 Global Application & Network Security Report*, The same report predicted that ransomware and DDoS for ransom schemes would continue to affect everything from traditional enterprises to cloud companies.

1 http://www.usatoday.com/story/tech/2015/06/24/fbi-ransomware-cyptowall/29215237/

Findings from the *Security and the C-Suite: Threats and Opportunities Report* underscore the validity of that prediction based on feedback from security executives. Radware conducted a survey of more than 200 C-level security executives form the U.S. and United Kingdom with the goal of understanding their greatest challenges, threats and opportunities when it comes to information security. Among those who have not experienced a ransom situation, the majority—77% in the U.S. and 91% in the U.K.—say they would not pay. Yet among those who actually experienced a ransom attack, response varies among U.S. versus U.K. executives. Interestingly, 64% of U.K. executives reported paying a ransom, more than double the 29% in the U.S. who said the same. For those who paid, the average ransom in the U.S. was $7,560 versus £22,218 among the organizations that paid attackers in the U.K.

Paying Ransoms

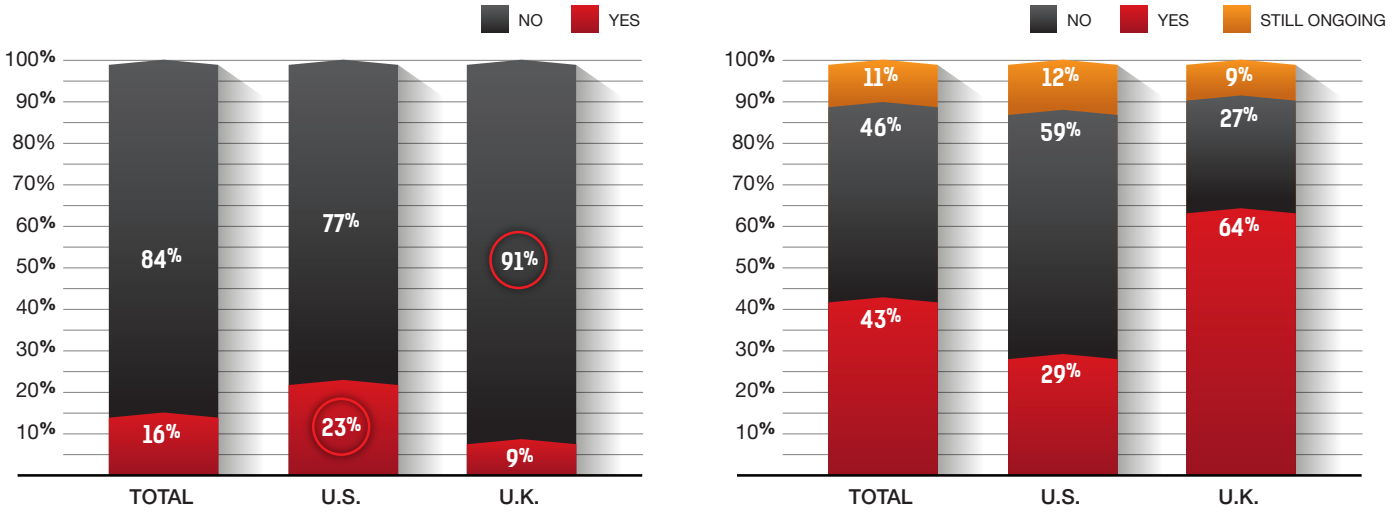

Figure 1: Paying Ransoms

Across industries and geographies, the propensity to send funds could reflect a strong desire to make the threat "go away" by simply giving in to the demands. That action may have the unintended—and undesirable—consequence of inviting continued ransom threats. If word gets out on the "dark web" that a company paid, it can expect to receive additional threats from the same or different attackers. After all, negotiating with criminals can become a proverbial slippery slope.

ProtonMail—the Swiss-based encrypted email provider – witnessed this firsthand. In November 2015, the company experienced consecutive attacks initiated with a ransom request by hacker group The Armada Collective. Hoping to stop the attacks, ProtonMail paid a ransom, only to see the attacks continue with volumetric and burst attacks combining application and network vectors.

The Kansas Heart Hospital in Wichita learned a similar lesson in May 2016. Having fallen prey to ransomware, the hospital paid the ransom to get its files back. Instead, it received only "partial access," along with a demand for more funds. The

Direction of Attack

Most cyber-attacks groups execute these ransom attacks via their own network stressers, however some leverage publically available stressers that are available via the "dark web." When experiencing a ransom attack, expect +100Gbps and multi-vector attacks simultaneously. Nor will these assaults be speedy. They're persistent and will often times last days or even weeks. Common attack vectors include the following protocols:

- SSDP
- SYN Flood/ACK
- DNS
- TCP RST/SYN
- UDP
- ICMP
- NTP

hospital declined the second request. Its experiences were the latest in a string of ransomware attacks targeting hospitals and health systems across the U.S. In addition to The Armada Collective, other groups have emerged at the forefront of this trend, including DD4BC and ezBTC Squad. One of the newest players is Kadyrovtsy (named after the elite forces of the Kadyrov administration in Chechnya), which recently threatened two Polish banks and a Canadian media company. Meanwhile, "copycats" are compounding the headaches. These players are issuing fake letters—hoping to translate empty threats into fast profits.

Next Steps

While it is impossible to predict the next target of a ransom group, organizations need to proactively prepare their networks and have an emergency plan in place for such an incident. If faced with a threat from a blackmail group, it is important to take the proper steps to mitigate the attack. Organizations under attack should consider:

- A security solution that can protect an infrastructure from multi-vector attacks, including protection from network and application-based DDoS attacks, as well as volumetric attacks that can saturate the Internet pipe.
- A cyber-security emergency response plan that includes an emergency response team and process. Identify areas where help is needed from a third party.
- Monitoring security alerts and examining triggers carefully. Tuning existing polices and protections to prevent false positives and allow identification of real threats when they occur.

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

How Can You Detect a Fake Ransom Letter?

- **Assess the Request**
  The Armada Collective normally requests 20 Bitcoin (approx. $6,000 US Dollars at the peak of the attacks), while other campaigns have been asking for amounts above and below this amount. Fake hackers request different amounts of money. Low Bitcoin ransom letters are most likely from fake groups who are hoping their price point is low enough for someone to pay rather than seek help from professionals.
- **Check Your Network**
  Real hackers prove their competence by running a small attack while delivering a ransom note. If you witness a change in your network activity, the letter and the threat are probably genuine.
- **Look for Structure**
  Real hackers are well organized. Fake hackers, on the other hand, don't link to a website. Nor do they have official social media accounts.
- **Consider Other Targets**
  Real hackers tend to attack many companies in a single sector. Fake hackers are less organized, targeting anyone and everyone in hopes of making a quick profit. Contact peers or information sharing organizations in your industry to see if there is a more widespread campaign underway.