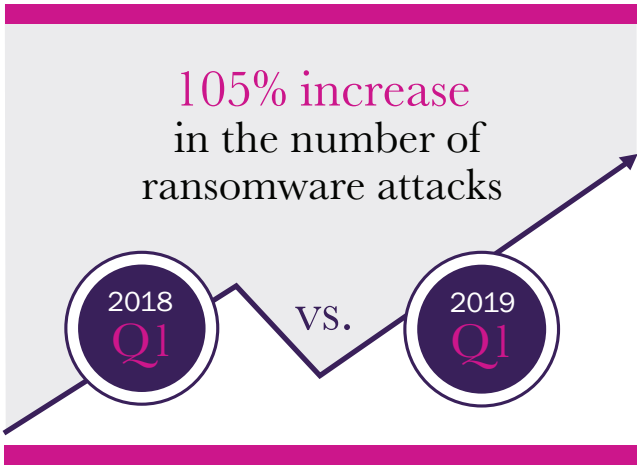
Ransomware attacks skyrocket, Q1 2019



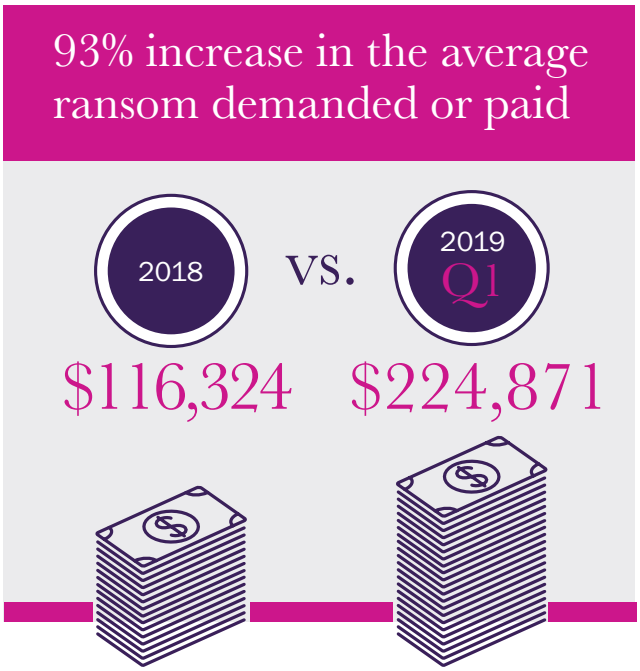
Ransomware attacks skyrocketed in the first quarter of 2019, according to the Beazley Breach Response (BBR) Services team, which reports a 105% increase in the number of ransomware attack notifications against clients compared to Q1 2018.

Not only has the frequency of attacks increased, but attackers are shifting focus, targeting larger organizations and demanding higher ransom payments.

While ransomware-as-a-service (RaaS) attacks remain commonplace and tend to hit unsuspecting small businesses, sophisticated attack groups associated with Ryuk and Bitpaymer ransomware variants are targeting larger organizations through phishing emails and tricking users into deploying banking Trojans.

In the first quarter of 2019, the average ransomware demand reported to the BBR Services team was 93% higher than the 2018 average. And, according to incident response firm Coveware, the average price of ransoms in Q1 2019 increased by 89% as compared to Q4 2018.

Bill Siegel, CEO of Coveware, attributes the increased number of attacks to two main factors. "First, anytime the average ransom demand goes up, it's going to pull in more attack groups interested in making money. Second, the easy availability of exploit kits (such as banking Trojans) and RaaS means there is a lower barrier to entry for would-be hackers."



While banking Trojans are not a new form of malware – first hitting BBR Services' radar in 2015 – within the last year, BBR services has seen a substantial increase in incidents involving both ransomware and banking Trojans. Banking Trojans were first designed to steal banking credentials from users of online banking websites. However, with recent variants such as Emotet and Trickbot, criminals have also been able to harvest all kinds of account credentials. Newer types of banking Trojans will also perform reconnaissance on email accounts and deploy other malware, most commonly ransomware, onto a system with relative ease. Cybercriminals exploit the stolen credentials to steal from financial accounts, defraud through business email compromise, or commit identity theft.

Today's banking Trojans are more dangerous and disruptive, and once infected, organizations have a hard time eradicating them from their network. It's more important than ever to prevent banking Trojans gaining a foothold and to respond quickly and effectively if they do.

BZCER022_US_05/19

Journey of a banking Trojan

1. A phishing email appears in the user's inbox. Often it will use stolen logos and design from a trusted financial institution or tech company. The email may simulate an alert about account activity and direct the victim to a fake web page or request urgent review of a Microsoft Office or PDF attachment.
2. Once the user clicks, a macro will launch to install or download additional malware. All too often, untrained users will click to enable macros to run if IT has not disabled the capability.
3. After installation, banking Trojans are adept at disguising themselves and establishing persistence.
4. Once one machine is infected, banking Trojans spread aggressively through the network. They will harvest any network credentials possible and use them to attack other systems on the network. They exploit unpatched Microsoft Server Message Block (SMB) vulnerabilities (like those involved in the spread of WannaCry) and harvest any personal credentials entered or stored on the system.
5. Stolen credentials aren't the only risk. Once established on an endpoint or a network, the Trojan can download other, more damaging malware.

If you think your system has been infected with a banking Trojan:

- Disconnect infected machines from the network (wired and wireless) as soon as possible and preserve them for forensic investigation.
- Reset passwords for any users of the machine and alert employees to change passwords for any personal accounts they may have accessed through the machine.
- Notify BBR Services to help obtain the expert services you need to investigate the incident and to determine whether data has been exfiltrated that gives rise to a legal obligation to notify affected individuals.

The war rages on as banking Trojans are proving themselves to be particularly hard to eradicate. In many cases, the initial response needs to be followed up by a second attempt to contain it as the malware has continued to spread through the network. There is no substitute for a strong education program combined with up-to-date and comprehensive risk management measures in place.

Businesses can help their people to stay alert to the risks with these simple measures:

- Alert employees to the current flood of phishing attempts using our employee training tip sheet on banking Trojans.
- Regularly train employees not to open unsolicited attachments and links, particularly from unknown sources; not to allow macros to run; and to be suspicious of links leading to web pages that ask for login credentials.
- Train employees not to store any personal login information on their computers, even through their browsers.

Banking Trojan names

About Beazley's BBR Services Team

Beazley has managed thousands of data breaches since the launch of Beazley Breach Response in 2009 and is the only insurer with a dedicated in-house team focusing exclusively on helping clients handle data breaches.

The BBR Services team works directly with BBR insureds during all aspects of incident investigation and breach response and coordinates the expert services that BBR insureds need to satisfy legal requirements and maintain customer confidence. In addition to coordinating data breach response, BBR Services maintains and develops Beazley's suite of risk management services, designed to minimize the risk of a data breach occurring.

beazley

www.beazley.com/bbr