State of Ransomware

Industry Update ANZ 2020

BlackBerry

The increased reporting of cyber incidents among large companies in ANZ in the first half of 2020 has been clearly evident. A handful of ransomware families are dominating these attacks. In this paper, we investigate some of the tactics used by these ransomware families, their high profile victims, and the strategies used to defend against these threats.

It is not uncommon for many organisations to fail to report breaches, or worse, to be completely unaware that they have even taken place. Ransomware is being used for much more than just blackmail. It can be used as a diversion; first harvesting credentials for later use, and then encrypting the drive to keep IT staff occupied while the attacker covers their tracks.

More recently, attackers have accomplished even more nefarious objectives, like sending critical data to the dark web, or auctioning it to the highest bidder.

It is not uncommon for many organisations to fail to report breaches, or worse, to be completely unaware that they have even taken place.

Everything as a service

Ransomware can be easily obtained and used by criminals that have little to no hacking skills, in what is known as Ransomware as a Service (RaaS). By establishing a network of affiliate partners, malware authors are able to spread their ransomware widely and scale earnings dramatically in the process.

Many threat actors have evolved from mass-volume consumer attacks, opting instead for more carefully planned and targeted attacks aimed at maximising disruption. By using a RaaS model, the authors of malware are significantly lowering the bar for launching such attacks, making this particular form of cybercrime accessible and profitable for a larger pool of potential criminals.

Many of our customers sought out BlackBerry because it is highly effective in preventing ransomware attacks. In each case, BlackBerry was able to analyse, predict and prevent the threat, with no updates required, on average over 1000 days before the malware was first discovered in the wild.

ANZ in the headlines

Toll Group, the Melbourne based global logistics company, has been hit twice by ransomware attacks in 2020 - in January by MailTo and in June by Nefilim. Also in June, government agency ServiceNSW, steel maker BlueScope, and a financial services company, MyBudget, all made the headlines due to high-profile cyber-attacks.

BlackBerry

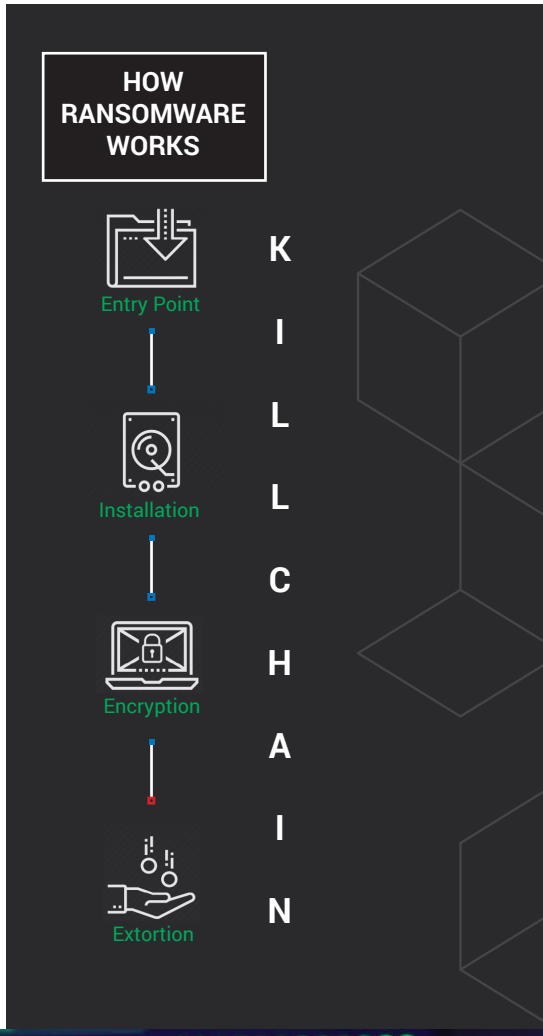
Anatomy of an attack – Emotet, Trickbot and Ryuk

There are a number of vectors ransomware can take to access a computer.

One of the most common delivery systems is phishing - attachments that come to the victim in an email, appearing as a file from a trusted source. Often clever social engineering is used to make the e-mail appear legitimate. Emotet, as an example, can scrape mail files and craft mail to colleagues using previous content. Emotet malware is typically used as a loader for TrickBot campaigns. Once loaded, TrickBot uses several modules to carry out various activities on the victim's system. It allows for lateral movement and enables utilities to be loaded manually by the operators. Once post-exploitation tools are loaded, the domain controller (DC) is attacked. When privileged access to the DC is acquired, Ransomware such as Ryuk can be deployed across the network at the botnet operator's will.

Another vulnerability that has been exposed is Remote Desktop Protocol (RDP). Used to enable remote access, RDP has a history of insecurity, leading to attacks either by brute force or exploitation. Perhaps the most infamous instance of ransomware, WannaCry, also took advantage of exploitable networking protocols.

Unfortunately, traditional defensive measures such as anti-virus agents are unlikely to stop ransomware, since the attacker can easily disable them.



BlackBerry®

True predictive prevention

Many of our customers sought out BlackBerry because it is highly effective in preventing ransomware attacks. The table below shows the BlackBerry advantage in relation to the most prominent ransomware families in ANZ. In each case, BlackBerry was able to analyse, predict and prevent the threat, with no updates required, on average over 1000 days before the malware was first discovered in the wild*.

	Phobos	Ryuk	Sodinokibi/ Sodin/ Revil	Zeppelin	Ako	Mailto	Nefilim	STOP/Djvu	Maze
First Discovered	Dec 2018	Aug 2018	April 2019	Nov 2019	Jan 2020	Aug 2019	March 2020	Dec 2018	May 2019
BlackBerry Advantage	1229 Days	1340 Days	1343 Days	1496 Days	1000 Days	1567 Days	1448 Days	1714 Days	1464 Days
Predecessor	CrySiS/ Dharma	Hermes	GandCrab	VegaLocker/ Buran/ Jamper/ Delphi	Medusa Locker (Sept 2019)	Netwalker, KoKo	Nemty	Brand new family	Brand new family
Deployment	Spam, RDP Creds	Spear Phish, Exploit	Oracle Weblogic, MSSP	MSSPs	RDP Exploit/ Stolen Creds	Phishing, DLL Injection	RDP Exploit	Cracks and adware	Email, RDP, Exploits
Targeting	In-discriminate	Large Businesses & Institutions	Large MSSPs & their customers	High profile victims via MSSP	Large Businesses and Institutions	Large Businesses & Institutions	Large Businesses & Institutions	In-discriminate	Large Businesses & Institutions
Crypto Algorithms	RSA1024+ AES256	RSA4096+ AES256	Curve25519+ Salsa20+ AES256	RSA4096+ AES256	RSA2048+ AES	Curve25519+ Salsa20+ ChaCha	RSA2048+ AES128	Salsa20	RSA2048+ ChaCha
Extensions	.phobos	.ryk	random	random	random	random	.nefilim	.djvu, .tro, others	random
Payment	0.1-2 BTC	15-50 BTC	5-300 BTC	unknown	$3,000	Varies	Varies + Exfiltration	~$1000	Varies + Exfiltration

Contact us to find out how to minimise the risks of a ransomware breach by transitioning from a reactive to a prevention-first security posture.

* source: SE Labs Report. BlackBerry acquired Cylance in February 2019. SE Labs conducted its study on the CylancePROTECT® solution, which is now known as BlackBerry® Protect.

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 175M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear - to secure a connected future you can trust.

BlackBerry. Intelligent Security. Everywhere.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

CONTACT US