

The Sandbox



How do we stop ransomware?

Satnam Narang, Tenable

Ransomware has been around for a while, with the first recorded instance in 1989 delivered via a floppy disk. Previous efforts to monetise malware were not without their challenges: however, the popularisation of cryptocurrency changed that dramatically. Today, it is now easier for attackers to make a profit from their efforts. Since the infamous WannaCry attack in 2017, ransomware continues to make headlines around the globe as attackers enjoy massive success at targeting organisations of all shapes and sizes. And this has emboldened them as they look to refine their attacks. CISOs should recognise that, as long as ransomware remains profitable for cyber criminals, it isn't going away.

In 2019, we've witnessed an explosion of ransomware attacks against myriad businesses, public sector organisations and non-profits. The cost of recovery and clean-up in conjunction with potential reputational damage and operational disruption mean that ransomware should be a top concern for CISOs today.

The most popular way attackers infect organisations is through spam and phishing emails. In the majority of cases, these messages include a malicious attachment, such as a Microsoft Word document or PDF file containing malware. Others, however, may contain a link to a web page controlled by the attackers. The goal is to get the target to open the attachment and trick the victim into enabling macros or clicking the link, which can then deliver a malicious downloader, leading to the final payload, which is ransomware.

In addition to spam and phishing emails, ransomware attacks exploit old, unpatched vulnerabilities. For example, the ransomware attack against the city of Atlanta in 2018 exploited a vulnerability in systems that remained unpatched for years. Another ransomware strain known as Satan took advantage of the same vulnerability used in the WannaCry attack, but also used flaws found in

Red Hat JBoss, Apache Tomcat, Oracle WebLogic and others. Attackers will actively search for software they know is flawed to exploit it in an attack.

To avoid falling victim to ransomware, organisations need to implement security awareness training and a vulnerability management programme. Security awareness training can help thwart the threat posed by malicious spam and phishing attacks. When it comes to vulnerabilities, it is important to observe that with the number of vulnerability disclosures constantly climbing, keeping on top of them can seem insurmountable. In 2018, 16,500 software vulnerabilities were reported, of which the majority were rated critical or high. However, of these 16,500, exploits were developed for just a small fraction. Knowing which vulnerabilities pose a real versus theoretical risk can empower CISOs and senior executives, leading them to concentrate efforts on the vulnerabilities that matter most.

While no-one knows how many ransomware attacks have gone unreported, it is safe to say that many of these attacks do, so the true scope of ransomware attacks is unknown. We expect ransomware to maintain its stronghold as one of the major threats affecting organisations going into 2020, as cyber criminals continue to refine their methods, including equipping themselves with new software vulnerabilities to leverage in their attacks. For CISOs, it's critical to know which applications and assets have vulnerabilities and which of these flaws are being exploited by attackers.

Organisations must ensure they're focusing on the vulnerabilities that are both dangerous and likely to be exploited, making the best use of their resources and increasing the return on their risk management investments. By implementing an effective risk-based vulnerability management programme, organisations can stay one step ahead of the attackers.

EVENTS

4–5 February 2020

PrivSec

London, UK

<https://london.privsec.info>

14–15 February 2020

Offensive Security

Berlin, Germany

www.offensivecon.org

24–28 February 2020

RSA Conference USA

San Francisco, US

www.rsaconference.com

16–20 March 2020

Troopers

Heidelberg, Germany

<https://troopers.de>

16–18 March 2020

ACM Conference on Data and Application Security and Privacy

New Orleans, LA, US

www.codaspy.org

17–18 March 2020

Cybersecurity & Cloud Expo Global

London, UK

www.cybersecuritycloudexpo.com

30 March – 1 April 2020

InfoSec World

Florida, US

www.infosecworldusa.com

7–8 April 2020

Global Privacy Summit

Washington DC, US

<http://bit.ly/2nLBsAy>

5–8 May 2020

RuhrSec

Bochum, Germany

www.ruhrsec.de

5–6 May 2020

Secure360

Prior Lake, MN, US

<https://secure360.org/secure360-twin-cities/>