SEQRITE

PREDICTIONS 2020
CYBERTHREATS

ABOUT

2020 is a challenging year for businesses, governments and civilians to fathom and deal with a new age of emerging threats. While victim entities along with their cybersecurity partners will be on toes to dynamically counter a large variety of threats, cybercriminals will be doing the same thing, leaving no stone unturned to outwit defenders.

Attackers are predicted to leverage a lot of AI in building a Guerilla warfare strategy to maximize the impact of their attacks and throw cyberdefenses off-balance. Apart from AI, legacy and new attack tactics are predicted to occur in 2020.

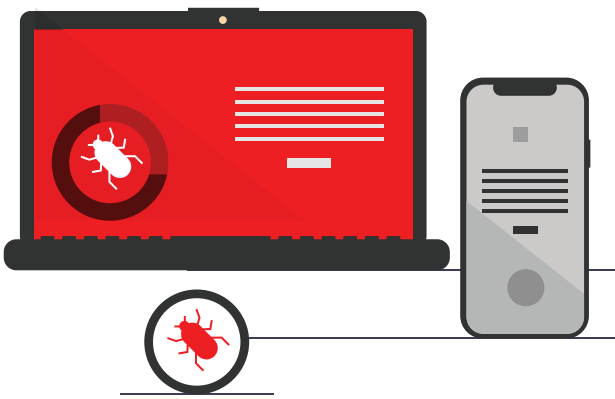
PREDICTIONS

1. Increase in Web Skimming attacks

Magecart proved to be a prominent web skimming attack in 2019 as well, with thousands of websites compromised to deliver skimming code. Similar to Magecart, Pipka is another web skimmer which has recently emerged having self-deleting code abilities. We suspect that skimming attacks are set to increase in 2020, as we see a huge number of hits for these attacks at this point in time.

2. Look out for more Bluekeep-like wormable exploits

Until now, publicly available exploit codes for Bluekeep could only achieve DoS attacks on the victim machine, but it's only a matter of time that attackers will figure out ways to exploit the vulnerability to its full potential and perform more severe attacks like delivering trojans and ransomware - authors of the latter are constantly on the lookout for such wormable exploits, as it makes lateral movement easier.

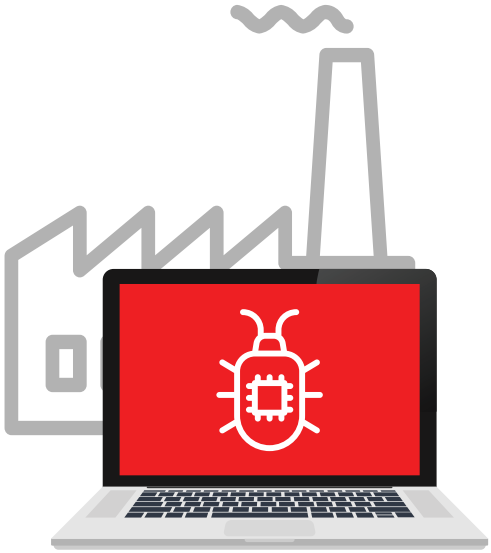


3. Deepfakes to cyber-frauds

Deepfakes are fake/manipulated video or audio clips of a person, created using deep learning technology. This can be used to create fake news and even carry out cyber frauds. A company's CEO featuring in a deepfake video asking colleagues or employees to transfer funds is a classic example of deepfake video.

4. APT attacks on critical infrastructures

The recent APT attack on Kudankulam Nuclear Power Plant has emphasized on the significance of security of the critical infrastructure. We may witness a rise in such APT attacks on the critical public infrastructure like transportation networks, power plants, telecommunication systems, etc. Such attacks can function in hiding for days, even months, stealing very large chunks of data before being detected.



5. Increase in threat landscape because of 5G

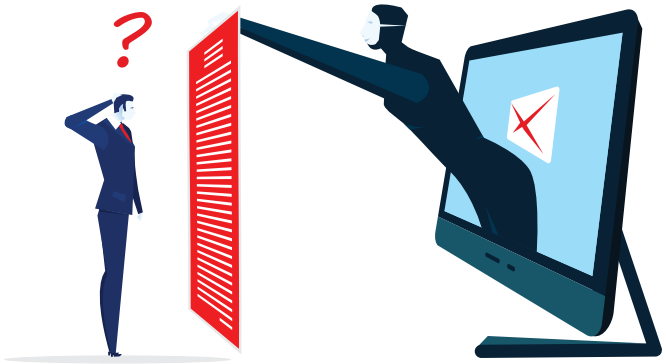
With 5G network, everything from your car to refrigerator will now have access to high-speed connectivity. This will, in turn, create more exposure to attacks and more potential entry points for attackers. Threat actors, organizations & institutions will have a larger landscape to monitor and the growth of the confidentiality and privacy threats will be unprecedented. Also, the main functions of 5G depend on software rather than the hardware which leaves it vulnerable to malicious attacks.

6. Attacks against Windows 7 to increase

Since Microsoft is ending its support for Windows 7 from January 14, 2020, technical support and software updates from Windows will no longer be available for users. In the last quarter, we saw 67% of attacks on Windows 7 itself, which will increase all the more in 2020 because security updates will not be available for Windows 7.

7. Increased use of LOLBins

Cybercriminals will increase the use of 'Living Off the Land' techniques to bypass traditional security tools and application whitelisting. They may adopt new techniques to bypass behavioural-based detections.



8. Increase in Office Macro-based attacks over office exploits

As Microsoft has taken many steps to block MS Office exploits in the newer version of Windows, it is hard to execute exploit code on Windows. Moreover, exploits are specific to application versions, but Macros will execute in all versions of MS Office. There are many open source obfuscator and Macro generation tools freely available to create a Macro-based payload. Many security vendors are also blocking a Macro execution but Excel Macro 4.0 is freely available to bypass these techniques.

9. Ransomware to darken the cloud

Apart from attacks on individual computers and critical infrastructure, ransomware will be directed towards the fairly nascent concept of data stored on the cloud. Cloud infrastructure has vulnerabilities which, perhaps, the attackers are aware of but aren't brought to the attention of respective cloud technology developers. Hackers will ensure exploiting the cloud to steal copious amounts of data.

Dr. Sanjay Katkar
CTO & Joint MD,
Quick Heal Technologies Ltd.

"2019, from a cybersecurity standpoint, was another challenging year full of evolving threats, large scale data breaches and major policy changes, affecting businesses of all sizes. The year witnessed an evolving threat landscape, with cybercriminals adopting the latest tools and technologies to outsmart the enterprise ecosystem. In 2020, we foresee the threat landscape become more challenging, as a large number of cybercriminals deploy AI to scale up their attacks. State-sponsored threat actors will increase their use and sophistication of AI algorithms, to scrutinize defense mechanisms and customize attacks targeted to vulnerable areas in the enterprise network. We also expect attacks like deep-fakes, APTs, web skimming and ransomware among others to take center stage in 2020."

Seqrite's ninjas at its Security Labs have analysed a great deal of the global threat landscape while preparing this discovery document. The findings are authentic and based on our own sources transforming this report as an information goldmine for enterprise stakeholders.

Further, to validate our claim, here are some of the 2019 attacks that came true, which Seqrite had predicted beforehand.

Increase in Web Skimming attack

The projected rise in ransomware attacks targeting utility infrastructure

An increase in targeted IoT – based attacks

Mobile landscape expected to become more threat prone in 2019

Rise in targeted attacks to exploit supply chain vulnerabilities

Data protection to become essential due to data-centric attacks

Cryptomining and cloud-based attacks to rise

SEQRITE

Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune 411014, Maharashtra, India.
Phone: +91 20 66813232 | Website: www.seqrite.com | Email: info@seqrite.com