Ransomware Operators Move Away from Bitcoin

The number of Internet of Things (IOT) devices has continued to grow at a rapid pace, however cybercriminals have yet to really take advantage of this outside of botnet assembly which is used in DDOS attacks. IOT devices are regularly found to have vulnerabilities, however, they are used in DDOS attacks. IOT devices are regularly found to have vulnerabilities, however, they are being increasingly targeted by ransomware operators as a means to achieve initial access vector to target networks.

In 2022, we expect attackers to explore IOT vulnerabilities in more creative ways and use this as an initial access vector to access target networks.

Purple is the New Red

Threat intelligence-led Red Teaming has become a global standard for organisations to improve their security postures, however, there has been a disconnect between those performing the Red Teaming and those defending against it (Blue Team). This results in missed opportunities for both teams to employ threat intelligence-led Purple Team practices throughout their operational and engineering lifecycles.

In 2022, we expect engineering teams to employ threat intelligence-led Purple Team practices throughout their operational and engineering lifecycles.

Business Email Compromise using Deepfake Voice

Business email compromise scams involve criminal organisations and typically involve the execution of a scam to gain funds. As Ransomware operators look to avoid law enforcement, we expect them to continue to explore new vectors to achieve initial access to target networks. One such area of focus will be the use of Deepfake technology to create convincing voice imitations of individuals in order to trick employees into making payments or changing the direction of funds.

In 2022, we expect more criminals to utilise the rapidly developing deepfake technology to accurately impersonate the voice of the executive or finance team member making the request. This is likely to be an increasing threat as more and more of those verification checks are now happening over the phone, this presents new opportunities for the criminals.

Business email compromise can be seen as a stepping point before entering the target organisation. We expect to see a strong social engineering aspect, with attackers reaching out to targets through social networking and instant messaging platforms.

In 2022, we expect cyber attackers to have an increasing focus on employee’s personal devices as a stepping stone before entering the target organisation. We expect to see an increasing social engineering aspect, with attackers reaching out to targets through social networking and instant messaging platforms.

Effort to Prevent Small Fails Turning into Mass Failure

In today’s connected world, a small outage or failure can have far-reaching consequences. In particular, affecting products and services that are critical to day-to-day life in many parts of the world. We have seen the effects of this in recent times, with widespread outages affecting the supply of goods and services in the financial sector. The global coronavirus pandemic is a key contributor to this, with closed borders and limited international travel hampering the ability for money mules to enter countries to retrieve stolen funds. As international travel once again becomes the norm, we expect mules to return and attacks to continue to evolve to suit.

In 2022, we expect there to be an increased focus on operational resilience across the financial sector. With a greater number of criminals using deepfake technology to trick employees into making payments or changing the direction of funds, we expect companies to invest in additional controls to prevent the success of these attacks.

Return of the Bank Heist

Bank heists have historically been a key contributor to the criminal organisations’ ability to access the funds they need to operate. The global coronavirus pandemic has been a key contributor to this, with closed borders and limited international travel hampering the ability for money mules to enter countries to retrieve stolen funds. As international travel once again becomes the norm, we expect mules to return and attacks to continue to evolve to suit.

In 2022, we expect more criminals to utilise the rapidly developing deepfake technology to accurately impersonate the voice of the executive or finance team member making the request. This may have previously been just a walk down the corridor in the office, however, as people continue to work remotely there will be an increased need to ensure that these requests are genuine.

Operational resilience is an area that is often talked about in the financial sector, however, we expect this to be challenged with a need to update incident response plans and increase controls to prevent the success of these attacks.

In 2022, we expect there to be an increased focus on operational resilience across the financial sector.

A Blurred Response

In 2022, we expect attackers to explore new avenues to attack using employee’s personal devices as a stepping stone before entering the target organisation. We expect to see an increasing social engineering aspect, with attackers reaching out to targets through social networking and instant messaging platforms.

This is likely to be an increasing threat as more and more of those verification checks are now happening over the phone, this presents new opportunities for the criminals.

In 2022, we expect attackers to explore IOT vulnerabilities in more creative ways and use this as an initial access vector to target networks.