SETTING THE TRAP

Aðalsteinn Jonsson *on how stolen devices are being used for phishing*

Cyber crime is usually thought of as a remote activity perpetrated entirely at a distance. While this is certainly the preferred approach for most criminals, many cyber attacks involve the use of stolen physical devices, which are exploited for further monetary gain. Recently we have seen a trend towards adversaries combining physical theft with remote tactics such as phishing. Stolen devices can yield direct access to personal information and contacts, as well as lending weight to emotional manipulation and exploitation.

I directly encountered this tactic when my partner Snjolaug was the victim of a combined attack. Her bag containing an iPad was stolen from a train during a holiday in Switzerland, and she was later targeted with a 'follow up' phishing attack. Six months after Snjolaug's iPad was stolen, she received a false text message impersonating Apple Support claiming that the device had been found. The cyber criminal had used the phone number she left in Apple's 'lost device' message feature to instigate the phishing attack.

This was a textbook example of the way cyber criminals use emotional manipulation as part of their attack strategies. Threat actors know that their victims will likely jump at the chance to recover a stolen device, overriding any second thoughts about clicking unexpected links. Coupled with the personal details harvested from the device, criminals can craft a very effective targeted attack.

Snjolaug was no exception and was happy to hear her device had been recovered. It was only when I took a closer look that I realised that, even though the front of the Apple Support message and iCloud activation page appeared genuine, the domain was illegitimate. Security researchers always have second thoughts about such things, but many victims will proceed without spotting the trap. But how do these criminals come by the tools to develop such convincing campaigns?

The truth is, it's becoming far too easy for individuals to launch attack campaigns thanks to the rise of phishing kits on the Dark Web – cheap and accessible starter packs for DIY cyber attacks. Usually, these kits include code for setting up a phishing site that can be uploaded once a domain has been purchased. All it takes is for an amateur criminal to Google search 'how to configure and stage a phishing attack', and they will find a set of step-by-step instructions to guide them.

A quick scan of our phishing kit database revealed several tools relating to iCloud services, including 'Find my iPhone', the iPhone pin code, Apple TV and Apple Support. It's well-known that people are far more trusting when they see brand names or logos they recognise, especially when they've already been in contact about a recent issue.

These phishing kits are becoming increasingly sophisticated. During an investigation of one of these kits, we discovered that the developer included software code that blocks access to all the files in the kit if the fake 'admin' file is opened. Any trespassers will therefore be caught out and not be able to further analyse the kit.

Market research reveals that the price of a kit to steal credentials from a stolen iPad is a mere $70. Anyone can become a cyber criminal for less than a $100, even with no technical knowledge.

In most instances of theft, it's normally a case of wrong place at the wrong time, rather than the individual being careless. But even so, there are precautions individuals and businesses alike can take to protect themselves from phishing attacks should the worst happen. While device encryption is a popular defence against exploitation in the event of loss or theft, evidence has shown us that criminals are now likely to use the device to launch a phishing attack instead of going after specific contents. After all, why spend time breaking into the device if you can get the necessary information from the owner with a few simple social engineering techniques?

CYBER CRIMINALS WILL OFTEN USE EMOTIONAL MANIPULATION AS PART OF THEIR ATTACK STRATEGIES

The main thing to remember is to not let your emotions cloud your judgement. Fear, hope, relief and desperation can result in individuals missing the indicators of deception, so keep a rational mindset. To identify a phishing attempt, it's worth starting with any URLs or website domains – they can quickly reveal whether the sender is genuine. On a corporate level, businesses must implement a layered security solution to block known threats at the email server, detect in real-time those evasive threats that get delivered to user mailboxes and automated incident response to quickly clean up attacks before users can fall victim to them.

If you receive communication from a brand and you're unsure of its legitimacy, it's always worth giving the company a call to confirm if the activity is genuine. When it comes to cybersecurity, no precaution is too much. Having your personal property stolen is terrible, but falling victim to cyber criminals using those devices is worse ●

Criminals can use the personal details harvested from a stolen device to craft a very effective targeted attack

Aðalsteinn Jonsson is Threat Researcher and Data at Cyren