RSA Conference 2019

BETTER.

Peer2Peer

High Speed, Low Drag: How Intelligence Teams Leverage Deep/Dark Web Data

P2P3-R09: High Speed, Low Drag: How Intelligence Teams Leverage Deep/Dark Web Data

Lance Cottrell, Chief Scientist, Ntrepid Corporation

High Speed, Low Drag: How Intelligence Teams Leverage Deep/Dark Web Data

Security professionals know that much of the information they need for indications of breach and trends in attack methodologies is already available on the internet—the problem is accessing it. In the Peer2Peer session "High Speed, Low Drag: How Intelligence Teams Leverage Deep / Dark Web Data," a mix of law enforcement, MSSP, legal, and security individuals discussed their experiences with gathering security related open source intelligence (OSINT).

Most of the participants use OSINT to find stolen credentials that confirm security breaches and go on to notify impacted users. Some also monitor the internet for trends in threats and new attack methods or tools.

It is very difficult to collect information on malware or credentials at first release because it is very valuable and tightly held. In general, older data is easy to find and collect, because the value of the data drops quickly after the first sale. The timescale for the information to become widely available ranges from days to weeks. Participants saw a trend toward easier collection of older data through off-the-shelf tools and services that automate this kind of collection. Unfortunately, the public dumps are often very old and contain repackaged information, rather than containing any new data.

Searching the more public malware sources will only discover the tools used by script kiddies. Advanced hackers hold their tools much more closely. They do not put them out publicly, using secure peer-to peer-chat applications, rather than public dark web forums, to sell the code. This move away from public dark web forums happened due to the rapid shutdown and takeover of several popular dark web marketplaces.

Unfortunately, the collected information is often misleading. A dump of credentials for a particular service may not be evidence of a breach, but rather of a phishing attack on users of the service. On the other hand, researchers can sometimes learn what they need even if they don't access the actual credentials. Merely seeing the description of the credentials naming your company can indicate a serious compromise.

Several participants talked about pushback from their employers against conducting OSINT. Even when credentials are found, many companies are sensitive about alerting customers. Even if the credentials came from phishing, rather than from a breach, the alert still causes negative impressions and negative impacts on the company. In addition, corporations often have rules against visiting criminal websites, which can further complicate investigations. In many cases, the sites you need to visit are actively blocked.

Legal liability also makes businesses and organizations unwilling to buy stolen data or credentials. Participants mentioned that sometimes they can receive this from others, including hired service providers, thereby reducing the culpability of the buyer.

We discussed the issue of whether to notify other businesses if you find their data during your investigations. Law enforcement participants said they do, because they have a duty to warn. Others said they would share with other companies in their XX-ISAC group or other security collaboration organization. They are concerned about revealing their activity and sources & methods to unknown third parties. Warning an unknown party or business could put the researcher's organization at risk or expose their activity to the criminals.

One participant talked about his success in penetrating a network of online criminals in a South American country. His four-person team was able to go from an initial set of twenty online groups discovered through completely public sources to seven hundred highly restricted groups over four months of full-time effort. There are layers upon layers of groups, with the more public groups providing links to more private layers of groups. This did cause a data volume problem, as they ended up having to handle about twenty thousand messages per day across all of their accounts.

He mentioned that one challenge is the rate at which the criminals set up and tear down these groups and group chats. They do this both to stay ahead of law enforcement and to push out other criminals who refuse to pay or otherwise violate the standards of the groups. There are even Google spreadsheets published by the criminals to keep track of bad actors in the groups and to follow their changing aliases.

The participants talked about the importance of hiding their identities during investigations using VPNs or other non-attributed IP addresses, like pre-paid cell phones or MiFi devices. They were concerned that they could suffer cyber or physical attack if they were identified as security or law enforcement people lurking in the discussions.

There seems to be a wide range in paranoia and sophistication among the criminals. Some would give advice to use VPN services where they could choose IP addresses in countries other than where they or their targets are located. That approach maximizes difficulty for law enforcement to track the connections. While some criminals seemed to use fake accounts for all of their activities, others were seen apparently using their real accounts. The use of true name accounts seems to depend on where the criminals live. If law enforcement in their country is very lax about that kind of activity, the criminals are much bolder and less careful.

Finally, the group talked about security of their operations and OPSEC. Human error is a major source of exposure in these kinds of investigations. One person has a checklist they follow every time to avoid error, like a pilot's preflight or landing checklist. Participants agreed on the importance of systems failing closed to prevent error, ensuring you never go out with your true IP address showing. Virtualization was also a popular approach to ensuring systems and networks were protected. This was particularly important to those that were actively collecting malware samples and frequently invested their own environments.

Finally, we talked about the trend of criminals moving from TOR hidden services toward secure one-to-one or group chat applications. Criminals have great difficulty policing their own spaces. Their challenge is to identify the bad actors within the larger population of cooperating criminals. It is gratifying to see them suffering with the same identification and authentication problems that the defenders must face.