TELESOFT

CASE STUDY

UNAUTHORISED CRYPTOCURRENCY MINING

INDUSTRY: Telecommunications
DEPLOYMENT: FlowProbe/TDAC

CUSTOMER CHALLENGE:

Telesoft's customer represents one of the largest Network Service Providers (NSP) in the world. After selecting Telesoft to provide carrier scale network visibility and analytics, the Network Security Team found unauthorised cryptocurrency mining on it's network.

As mining is a computationally intensive process, cyber criminals had hijacked critical infrastructure within the network to steal computer power for mining operations.

If allowed to continue, this illegal activity on our customers network would negatively impact upon network performance and bandwidth capacity, reducing their ability to deliver revenue generating services.

DEPLOYMENT — FLOWPROBE/TDAC

1. What is Cryptojacking?

Cryptojacking is the running of unwanted applications on endpoints and infrastructure, specifically crypto currency mining software, and it's hard to detect. The cypto miner steals processing capability, resulting in higher electricity (power and cooling) consumption, slower performance of legitimate applications or services and a high CPU run rate generates more heat and reduces lifetime.

Cryptocurrencies are mined using complex mathematical calculations and require high processing power. An effective way to implement this is across a distributed network of nodes that perform individual calculations. One zero cost way to build such a network of nodes is to inject unauthorised mining software onto unprotected devices (phone, IOT device, laptop, tablet, anything with processing capability and an IP address), through an infected web url, email malware, deliberate insider installation or any hijacking technique. The node will then perform the calculations for free.

HEADQUARTERS
Telesoft Technologies Ltd
Observatory House, Stour Park
Blandford DT11 9LQ UK
+44 (0)1258 480880
+44 (0)1258 486598
sales@telesoft-technologies.com

AMERICAS
Telesoft Technologies Inc
430 National Business Parkway
Suite 480, Annapolis Junction
MD 20701
USA
salesusa@telesoft-technologies.com

ASIA
Telesoft Technologies Ltd
Tapasya Corp Heights
Ground Floor, Sector 126
Noida, 201301
+91 120 612 7725
salesindia@telesoft-technologies.com

2. How can TDAC and FlowProbe help to detect Cryptojacking?

Infected nodes need to communicate data, such as results of hash functions to other nodes and also send results to a control server or wallet. The actual messages communicated are usually very short and can be disguised as regular network traffic, making detection at the endpoint complex.

That means that the best way to detect cryptojacking is to monitor the network for suspicious activity, where a number of devices or nodes are likely to be exhibiting the same anomalous behaviour. Even though usually obfuscated, there can be patterns, such as packet size, port or period between communication sessions, or a pattern of uploading slightly more data than was downloaded.

Using the Telesoft FlowProbe for unsampled, multi 100Gbps, ultra high rate flow monitoring, in conjunction with the collection and analysis system ("TDAC"), the NetOps team within the NSP can discover anomalous traffic patterns which indicate cryptojacking activity. This allows corrective action to be taken to block unauthorised crypto traffic flowing through the network.

SUMMARY

Telesoft solved large scale cryptojacking using a multi-layer security strategy, deploying our cyber defence tools, to give total network visibility, enabling Network Security Operations (NetOps) teams the ability to drill down in to their network data to uncover damaging and illegal activity. Were it not for the combination of the multi 100Gbps FlowProbe with enriched L7 visibility and the monitoring and analysis platform (TDAC software), this exploit could have gone unnoticed, compromising our customers' ability to deliver their services.