Enriching Threat Intelligence for the Carbine Loader Crypto-jacking Campaign

team-cymru.com/blog/2021/07/08/enriching-threat-intelligence-for-the-carbine-loader-crypto-jacking-campaign/

S2 Research Team View all posts by S2 Research Team July 8, 2021

Co-authored by Andy Kraus and Dan Heywood

Cloud security provider Lacework published an article in April 2021 on a crypto-jacking campaign they dubbed “Carbine Loader”. The campaign targeted servers running Nagios XI, an enterprise network monitoring application.

Despite there being roughly 10,000 vulnerable public-facing Nagios servers, the campaign’s Monero wallet contained only around $900. This seemed a curiously small amount, particularly considering the campaign’s relatively sophisticated elements, such as the overwriting of logs and automated lateral movement.

We decided to take a look using our threat reconnaissance platform, Recon, to see what we could find out about the activity. The summary of our process is outlined below:

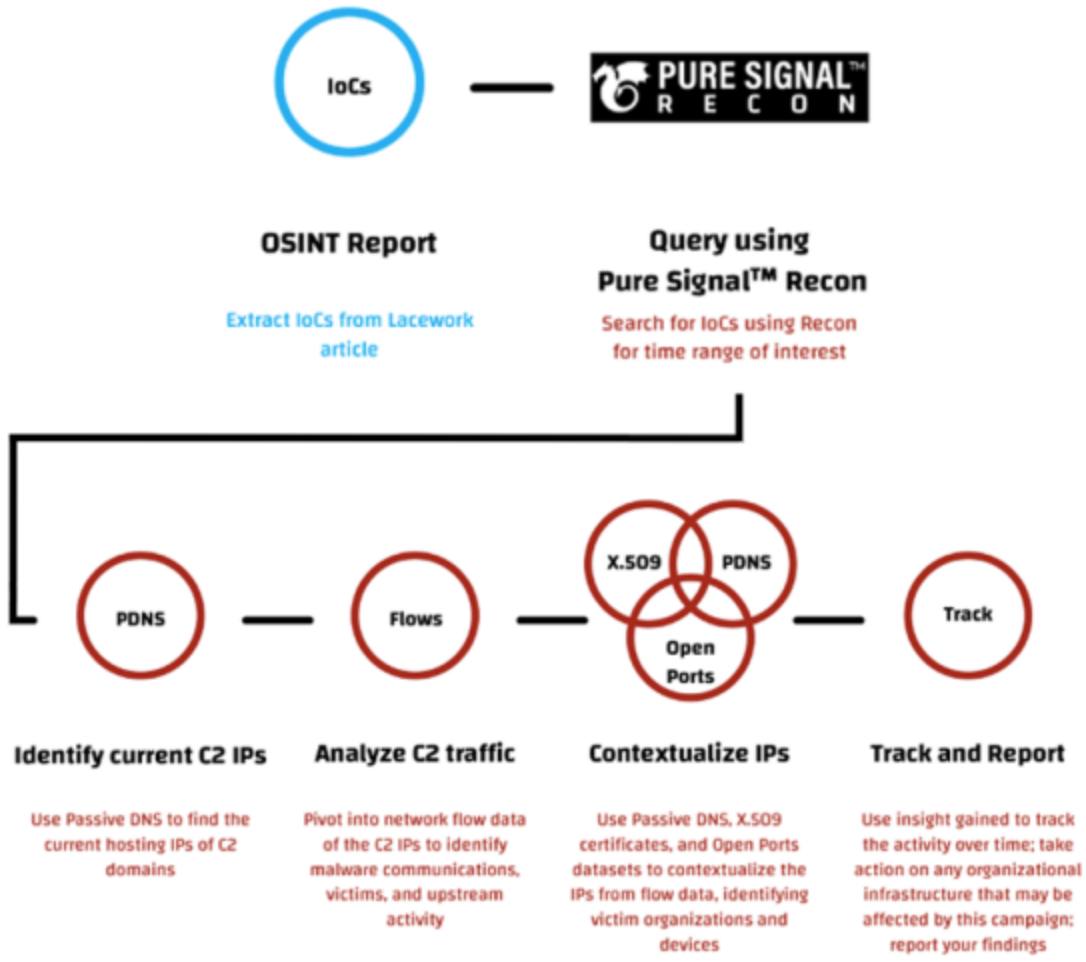

Figure 1: Process used to enrich the Lacework article

Passive DNS

Lacework detailed the use of two domains for command and control (C2) purposes:

1.) sslcer.justdied.com

- Infected hosts are set to beacon every 20 minutes to TCP/8080
- The mining server is hosted on TCP/3333

2.) jquery-dns-07.dns05.com

Used by related loaders as a C2 server

Using the passive DNS dataset in Recon, we confirmed Lacework's findings that the domains were primarily hosted on two IP addresses from January to the present.

Network Traffic

Based on the hosting information identified, we used Recon to pivot into our network traffic data to look for organizations communicating with the IPs.

Within this data set we were able to observe the expected traffic over TCP/3333 and TCP/8080, as specified based on analysis of the malware. In addition, we also saw traffic over TCP/445 and TCP/3389, originating from potential victim organizations.

Note: The TCP/445 and TCP/3389 traffic was sourced from IP addresses which also made connections to the C2 over TCP/3333 and/or TCP/8080.

X.509 Certificates and Open Ports

Pivoting into our X.509 certificate and Open Ports data sets, we could show that most of the IP addresses communicating with the two C2 servers were running Nagios XI by looking at the HTTP responses.

Many of these servers were found to be hosting the standard login page for Nagios devices.

Victimology

A review of our analysis showed 104 unique IPs communicating with the C2 servers. From these IPs, we were able to identify 31 distinct organizations based on enrichments from a variety of datasets in Recon, including Whois, ASN, PDNS, X.509, and Open Ports.

While one might expect a crypto-jacking campaign to be purely opportunistic (i.e., the more victims the better), the victim set we discovered seemed to have a focus on a few specific industries, including IT / Software and Higher Education.

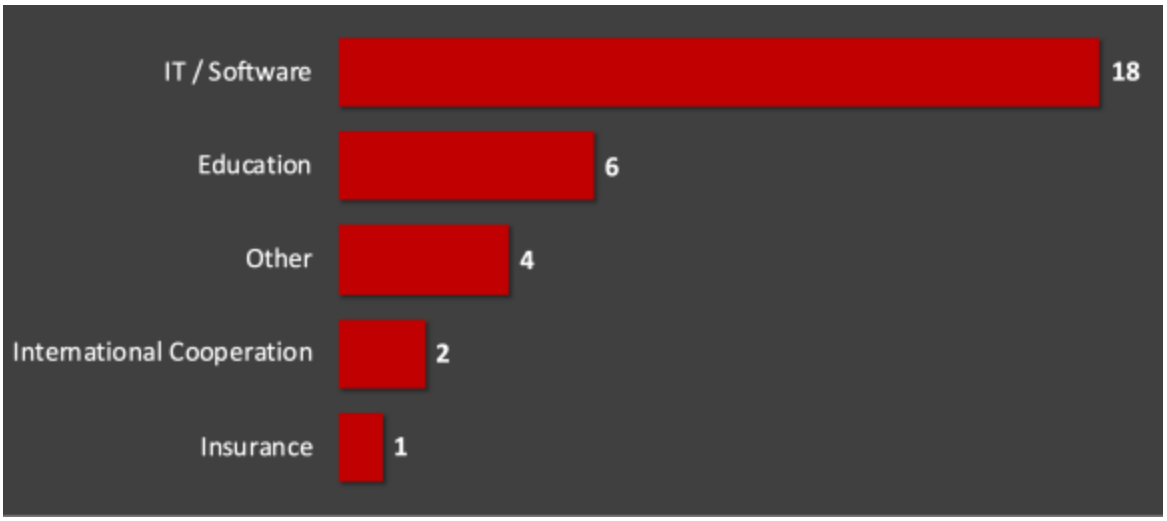

Figure 2: Identified victims by sector

In addition to the inbound command and control traffic, our network traffic data showed outbound TCP/80 and TCP/443 connections from the C2s to over a dozen additional organizations, activity which we attributed to potential reconnaissance by the threat actors. The organizations subject to this activity included an aerial imagery company, a financial software company, an agricultural agency, and an educational establishment.

Financials

Finally, we took another look at the threat actor's Monero wallet in early June and the value was still approximately the same (2.7 XMR vs. 3.12 XMR) as Lacework reported.

The campaign currently has no active miners operating, despite ongoing beaconing from victims to the C2s.

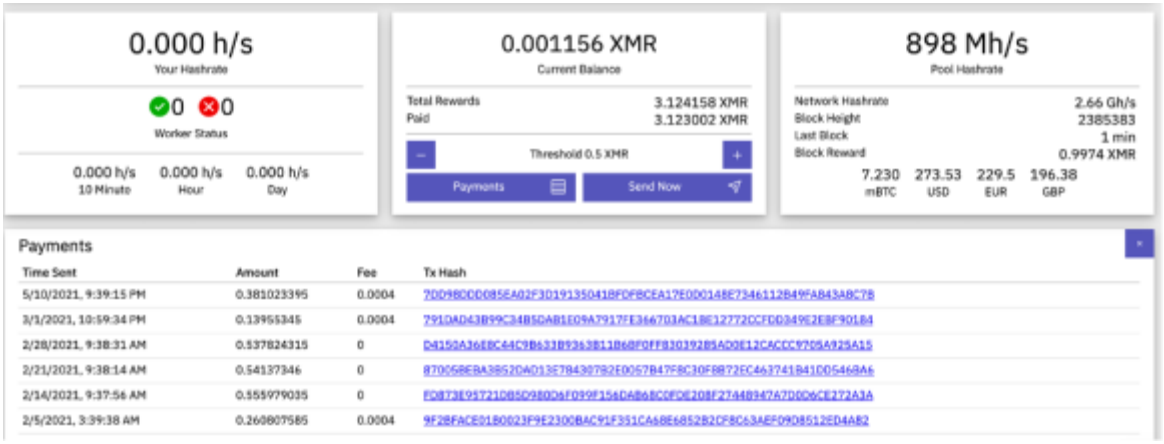

Figure 3: Monero wallet used by the threat actors

Conclusion

Using Recon, we were able to build on the excellent analysis provided by Lacework and in the process identify a possible evolution of malware communications via TCP/445 and TCP/3389, based on our ability to track the hosting IP addresses of C2 domains (and

potential victims) over time.

While on the surface this appears to be standard crypto-jacking activity, the content of the crypto wallet and victimology seem to tell a different story. While we can’t come to any definitive conclusions at this time, there may be more to Carbine Loader than meets the eye.