PRTG: Helping a Leading Independent Security Analyst Detect and Prevent Cryptojacking

> "As with all things in IT, visibility is key. If you see a server running at peak capacity for no reason, you immediately know there's a problem. You can't account for, let alone combat, threats you can't see or don't know of. PRTG isn't a security tool, but it's my favorite compliment to them. Besides monitoring malware and botnets, I also use it to monitor phishing sites, which I find and report to the hosting provider."
>
> Troy Mursch

Many believe that cryptocurrencies will serve as the financial underpinning of an increasingly global economy. Bitcoin is the most widely known, but there are hundreds of similar digital currencies or altcoins as they are sometimes called.

Monero, an open source cryptocurrency that was launched in 2014 is one. Anonymous and untraceable, it works much like small bills in a traditional open market. Other popular cryptocurrencies, or tokens, include Dash, Ethereum, Litecoin and Ripple - all of which provide a global standard that avoids the need for a centralized bank.

While numerous regulatory hurdles remain, the use of cryptocurrencies is increasing, spurred on in part by the fact that they enable faster transactions than more traditional means of finance. But the move to digital currency is not without challenges.

Blockchain, Cryptomining and the Crime of Cryptojacking

The underlying technology on which cryptocurrency is based is blockchain. With cryptography to ensure that privacy is maintained, blockchain acts as a public ledger - a public database spread across multiple computers. Every time a transaction or asset is sent to another member, a block of data is created. And because the block is shared with every member, but remains encrypted, the integrity of the transaction or the movement of the asset can't be tampered with. In other words, there's no way to "cook the books" because every member receives every block and in that way possesses the entire ledger.

Of course, the underlying cryptography and complex mathematical algorithms required to make this happen require massive computing power, such as when adding transactions to the blockchain or verifying them. Miners are the computers that complete these complex computations, and in payment for solving them first they receive newly created cryptocurrency. This cryptomining is the digital equivalent of the minting process.

PRTG NETWORK MONITOR

TROY MURSCH'S NETWORK MONITORING TIPS:

- ✓ Remember that without monitoring you are flying blind.
- ✓ Always be on the lookout for malware, whether it's cryptojacking-oriented JavaScript or an executable that impacts your servers.
- ✓ Use remote probes. It's important to look at your network from outside and inside.
- ✓ Use the non-security oriented data you get from your monitoring efforts to improve your network infrastructure and provide your users with greater service.
- ✓ Monitor, monitor, monitor...today's increasingly complex networks require constant vigilance. You always want to be the first to know when a problem arises.

Not surprisingly, cyber criminals are drawn to the money-making potential associated with mining – something Troy Mursch, an independent security researcher and creator of the Bad Packets Report, a website devoted to research on cryptojacking, botnets and other security topics, knows all too well. Mursch is not only the leading researcher on cryptojacking malware, but is also one of the most experienced professionals when it comes to helping companies, including numerous small and medium-sized businesses, detect and combat cyber threats like cryptojacking. Few people know more about the impact it can have on infected computers and mobile devices.

"Cryptojacking typically happens after a website is compromised to inject cryptojacking malware. In most cases this malware is merely a few lines of JavaScript," says Mursch. "Once it's placed on the website, visitors to the site immediately begin mining cryptocurrency on behalf of the cybercriminal who placed it there. It can also be delivered in the form of an executable that targets servers rather than clients, but in both cases the outcome is the same: computing resources are hijacked by the malware, which directs CPU capacity to the mining process. And of course, all newly minted cryptocurrency – typically in the form of Monero that can't be tracked – is then sent to the cybercriminal's account."

Using PRTG to Detect Cryptojacking Malware

Last year Mursch was the first security researcher to discover cryptojacking malware on two very popular websites – CBS's Showtime, and Politifact, a Pulitzer Prize-winning site that verifies the accuracy of politicians' claims. Both were infected with Coinhive, which immediately commandeered 60 percent or more of visitors' CPU capacity to mine Monero.

He also discovered a similar scheme that infected around 1,500 websites with a copy of the Coinhive cryptocurrency miner that was hidden in the JavaScript files used by LifeHelpNow, a live chat and customer support widget. Most of the sites infected were online shops or the homepages for private businesses.

In each case, Mursch used Paessler's PRTG Network Monitor to find the offending malware. With an on-premises deployment and PRTG in the Cloud, and using an HTTP Advanced sensor and remote probes, he was able not only to find the offending code but also to confirm when it was successfully removed.

"I've used PRTG to find and combat many high-profile cryptojacking incidents and a simple HTTP Advanced sensor is really all you need to monitor affected websites," notes Troy. "It confirms the malware is there, tells you when an affected site is cleaned up, and confirms how long it was infected for. And perhaps most importantly, you can do all of this without going through the trouble of visiting a website that's infected with malware."

A System Administrator's Nightmare

Mursch cautions that cryptojacking is a serious issue that all system administrators, particularly those that serve small and medium-sized businesses, should take very seriously. He recently used PublicWWW, a search engine that indexes the entire source code of websites, to gauge the seriousness of the problem.

What he discovered was disturbing. Mursch found more than 48,953 sites infected with cryptojacking malware, 7,368 of which were WordPress sites used primarily by small businesses.

“In addition to impacting consumers’ trust, or in the case of executables impacting businesses’ servers, the impact is always the same. Cryptojacking takes existing CPU resources and funnels it to the mining process. Given that some of these mining operations take place over months, affected businesses and consumers will see higher electric bills, far more wear and tear on hardware, lost productivity due to slow-performing networks and in some cases serious physical damage to devices,” he says. “Mobile phones and tablets are particularly susceptible because they aren’t designed to run at peak CPU capacity for extended periods of time. When infected with cryptojacking malware, they can literally burn themselves up if left on a charger.”

Of course, all of this is further complicated by the fact that some websites are increasingly inserting Coinhive into browsers, and openly asking for visitors’ consent as a legitimate way to generate revenue in exchange for content, gaming or other services – something Information Technology (IT) departments will increasingly need to address with policies that safeguard their IT infrastructure.

“As with all things in IT, visibility is key. If you see a server running at peak capacity for no reason, you immediately know there’s a problem. You can’t account for, let alone combat, threats you can’t see or don’t know of. PRTG isn’t a security tool, but it’s my favorite compliment to them. Besides monitoring malware and botnets, I also use it to monitor phishing sites, which I find and report to the hosting provider.”

Liability is another issue. With more cybercriminals launching cryptojacking campaigns that target hundreds and even thousands of websites simultaneously, Mursch feels it’s only a matter of time before the liability for cryptojacking becomes a serious issue.

“If your customer’s mobile device fails because it overheated while cryptomining without their consent because they visited your e-commerce site, it wouldn’t be inconceivable for them to look for compensation,” adds Mursch. “Most importantly, they might not want to visit your site again.”

For more information on cryptojacking, botnets, network abuse and other security topics, visit Bad Packets Report at www.badpackets.net. Mursch has also coauthored a peer-reviewed research paper, “A first look at browser-based cryptojacking” which further explains the topic in detail.

ABOUT PAESSLER AG

Paessler AG’s award winning PRTG Network Monitor is a powerful, affordable and easy-to-use Unified Monitoring solution. It is a highly flexible and generic software for monitoring IT infrastructure, already in use at enterprises and organizations of all sizes and industries. Over 200,000 IT administrators in more than 170 countries rely on PRTG and gain peace of mind, confidence and convenience. Founded in 1997 and based in Nuremberg, Germany, Paessler AG remains a privately held company that is recognized as a member of the Cisco Solution Partner Program, the HPE Partner Ready Program, the NetApp Alliance Partner Program and VMware’s Technology Alliance Partner program.

PRESS CONTACT

Paessler AG
press@paessler.com
T: +49 911 93 775-0
F: +49 911 93 775-409

Lewis PR
paessler@teamlewis.com
T: +1 603 321 4710

Paessler AG
www.paessler.com
info@paessler.com