Infrastructure Analysis of Lazarus Group Attacks on Cryptocurrency

Published: 2017-12-20 · Archived: 2026-04-05 12:40:04 UTC

The Wayback Machine - https://web.archive.org/web/20171223000420/https://www.riskiq.com/blog/labs/lazarus-group-cryptocurrency/

Mining Insights: Infrastructure Analysis of Lazarus Group Attacks on the Cryptocurrency Industry

December 20, 2017, Yonathan Klijnsma

RiskIQ collaborated with Proofpoint Cyber Security on research for a report published today investigating the activities of North Korea's Lazarus Group, which highlights the group's recent focus on cryptocurrency investors and exchanges. Earlier this year, the activities of the Lazarus group in South Korea were discussed and analyzed, as they managed to compromise accounts on various South Korean cryptocurrency exchanges. More recently, they were seen targeting a United Kingdom-based cryptocurrency exchange. In this blog, we will show and explain our analysis of the infrastructure used in the attack described in the Proofpoint report.

The Start: Lazarus Group's IDN Phishing for Infections

In early November, Proofpoint uncovered a large active phishing campaign that sent out messages about fake Bitcoin Gold (BTG) wallet software. The actors abused IDN registration attempting to impersonate the official bitcoingold.org website using sender IDN domains and the decoded notations. Below are four examples of domain names registered for this campaign:

IDN version	Decoded version
xn--bitcoingod-8yb.com	bitcoingoľd.com
xn--bitcoigold-o1b.com	bitcoiņgold.com
xn--bitcoingld-lcb.org	bitcoingöld.org
xn--bitcingold-hcb.org	bitcöingold.org

The domains shown above appeared in our crawl data, meaning we had a full copy of the webpage and any metadata present on it. We'll take a look at xn--bitcingold-hcb.org which, in our data, looked identical to the genuine site:

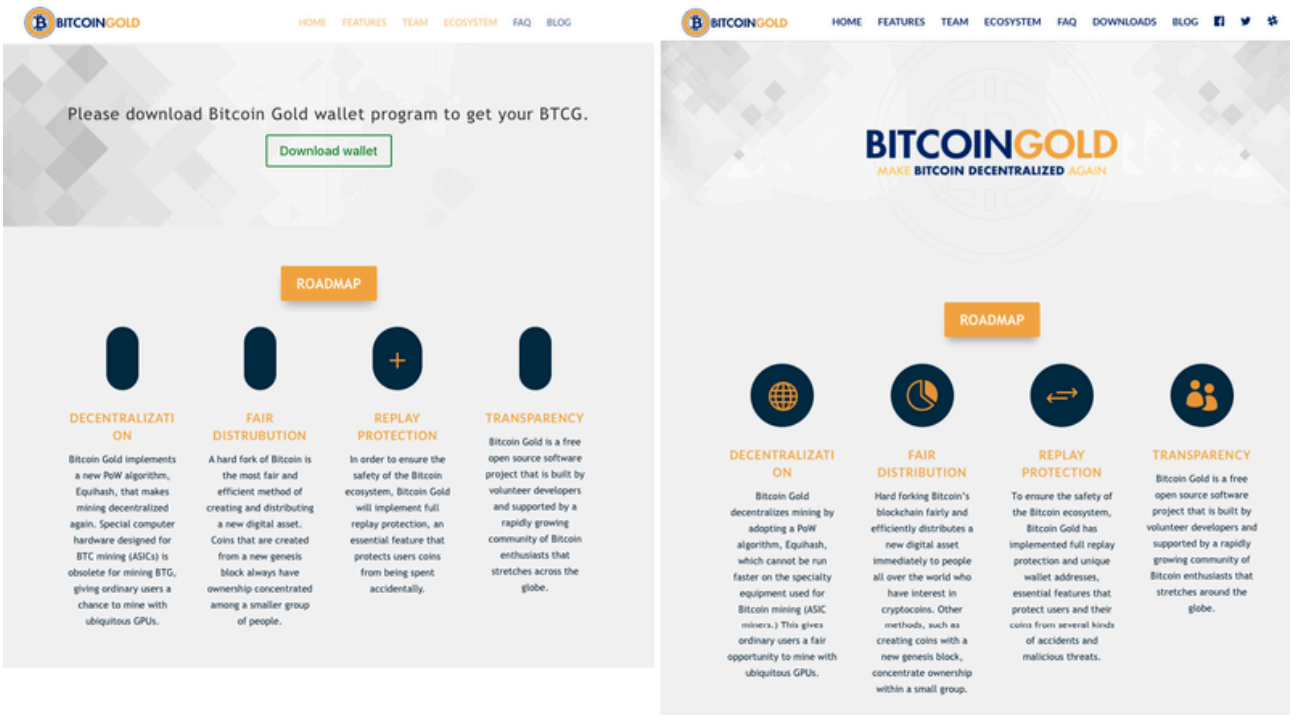

Fig-1 Fake site looks just like the genuine

Above, the fake page set up by the Lazarus group is on the left. Note the download button and pushed down 'Roadmap button,' which do not appear on the official site on the right, which has a logo and roadmap button instead. The actors copied the index page from the official Bitcoingold website and modified it, but they still link to the CSS, Javascript, and image resources of the official website, which we can see in the source of the page:

Fig-2 DOM captured by RiskIQ crawlers

The information above is really valuable to our investigation. As RiskIQ stores host pairs for sites that point to each other in a parent or child relationship. We can call upon this data set for the official Bitcoingold website and see at least two of the fake websites in its parent Host Pair set:

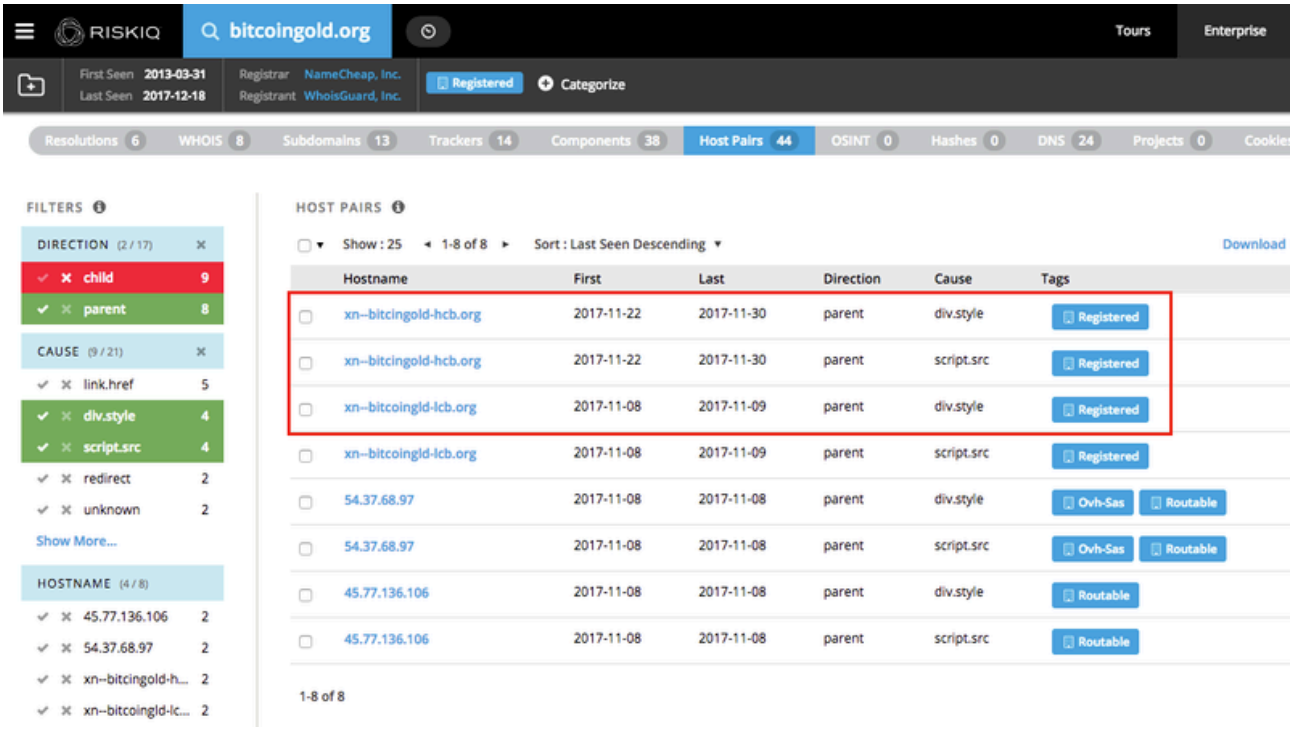

Fig-3 Host Pair data set inside RiskIQ PassiveTotal

Note: *We filtered on parent relationships to see hosts that pointed to bitcoingold.org, not hosts bitcoingold linked to itself.*

As reported by Proofpoint, the “download” button linked to a backdoored PyInstaller installation that was set up to download a version of the PowerRatankba implant. The button was linked via an onclick event to a JavaScript function:

```
<div class="et_pb_button_module_wrapper et_pb_module et_pb_button_alignment_center">
    <h2>Please download Bitcoin Gold wallet program to get your BTCG.</h2>
</div>

<div class="et_pb_button_module_wrapper et_pb_module et_pb_button_alignment_center">
    <button class="et_pb_button" style="color: green; border-color: green;cursor: pointer" onclick="download()">Download wallet</
    button>
</div>
```

Fig-4 Button linking to an onclick event

The invoked script redirects the user to the file download:

```
    <script type="text/javascript">
     function download(){
         location.href = 'https://bitcoingöld.org/bitcoingold.exe';     }
    </script>
```

Fig-5 The file download

The file downloaded here was seen with the following SHA256 hash:
eab612e333baaec0709f3f213f73388607e495d8af9a2851f352481e996283f1

Besides Bitcoingold, the Lazarus group performed the same kind of IDN ‘attack’ against the Electrum Bitcoin wallet website. The actors created the IDN website, xn--electrm-s2a.org, to serve as a fake software installation

page similar to the Bitcoingold clone:

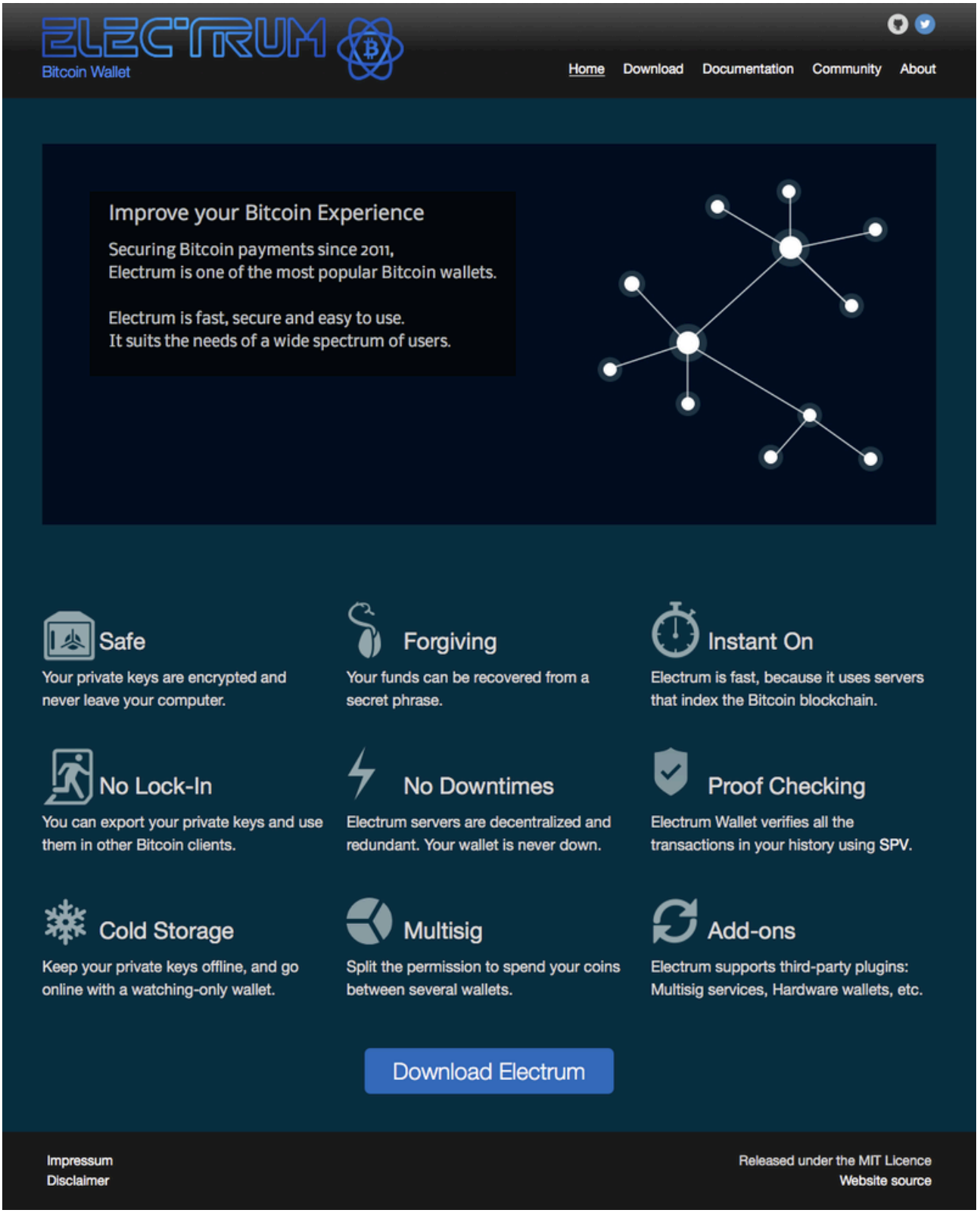

Fig-6 Similar attack on the Electrum exchange

Interestingly, Lazarus left some information in the source of the page that shows that they used the 'HTTrack' website copier tool, as well as the date (Friday, November 17th at 03:27:29 GMT as per our crawl data) they

copied the Electrum website:

Fig-7 DOM captures showing some interesting info left behind by Lazarus

Conclusions

Defenders with access to internet data collected by crawlers can detect unknown threats at the source and track how they change and spread. Correlating threat data extracted from a broad set of data sources across channels reveals the risk posed to an organization by a single piece of infrastructure—and how it's used within a broader context. As can be seen from the above analysis, RiskIQ's crawling infrastructure, indexed web data sets, and analyst-focused analysis platform allows organizations to quickly and effectively identify the scale of these strategic compromises and provide visibility that improves an organization's ability to defend their network.

Interested in crawling specific parts of the Internet with RiskIQ technology? Now you can task our virtual users to work for you at scale. RiskIQ offers URL crawling through our Security Intelligence Services (SIS), so you can capture the same kind of data we used in this post. For more information and a quote, contact us today.

Indicators of Compromise (IOCs)

The following IOCs are those found by pivoting around the known hosts from the phishing emails and expanding our list this way. We have some suspected hosts that are potentially related to this campaign, but we don't have proof (yet), these are not listed, but we will keep an eye out for any confirmed activity.

Below list does not include IOCs obtained from Proofpoint's malware analysis, those are available in their report or from the full list of IOCs is available in our RiskIQ Community Project: https://community.riskiq.com/projects/03e1e06f-4644-3b0e-7721-682b928d2001?guest=true&_ga=2.250911174.117879041.1513562791-1318539965.1474487244

Domain
xn--electrm-s2a.org
xn--btcongold-g5ad.com

xn--btcongold-54ad.com
xn--bitcoingod-8yb.com
xn--bitcoingld-lcb.org
xn--bitcoigold-o1b.com
xn--bitcingold-hcb.org
xn--bitcin-zxa.org

Source: https://web.archive.org/web/20171223000420/https://www.riskiq.com/blog/labs/lazarus-group-cryptocurrency/