SOHO PHARMING

A Team Cymru EIS Report: Growing Exploitation of Small Office Routers Creating Serious Risks

Powered by Team Cymru's Threat Intelligence Group

www.team-cymru.com

EXECUTIVE SUMMARY

Summary

This report details our recent analysis of a widespread compromise of consumer-grade small office / home office (SOHO) routers. Attackers are altering the DNS configuration on these devices in order to redirect victims DNS requests and subsequently replace the intended answers with IP addresses and domains controlled by the attackers, effectively conducting a Man-in-the-Middle attack.

As the bar is increasingly raised for compromising endpoint workstations, cyber criminals are turning to new methods to achieve their desired goals, without gaining access to victims' machines directly. The campaign detailed in this report is the latest in a growing trend Team Cymru has observed of cyber criminals targeting SOHO routers.

- In January 2014, Team Cymru's Enterprise Intelligence Services began investigating a SOHO pharming campaign that had overwritten router DNS settings in central Europe. To date, we have identified over 300,000 devices, predominantly in Europe and Asia, which we believe have been compromised as part of this campaign, one which dates back to at least mid-December of 2013.

- Affected devices had their DNS settings changed to use the IP addresses 5.45.75.11 and 5.45.75.36. Our analysis indicated that a large majority of affected routers resided in Vietnam. Other top countries affected included India, Italy and Thailand.

- Analysis of the victim devices affected revealed that the compromise is not limited to a single manufacturer. A range of router models from several manufacturers appears to be compromised. As with the DNSChanger malware, unwitting victims are vulnerable to a loss of service if the malicious servers are taken down, as both primary and secondary DNS IP addresses are overwritten, complicating mitigation.

- The affected devices we observed were vulnerable to multiple exploit techniques, including a recently disclosed authentication bypass vulnerability in ZyXEL firmware and Cross-Site Request Forgery (CSRF) techniques similar to those reported in late 2013.[1]

- This large-scale attack has similarities with a recent, highly targeted attack against Polish consumer bank customers, though subtle differences in tradecraft point to these being separate campaigns.[2] We also believe that this activity is separate from the Linksys Moon worm recently reported by the SANS Institute.[3]

- We assess that consumer unfamiliarity with configuring these devices, as well as frequently insecure default settings, backdoors in firmware, and commodity-level

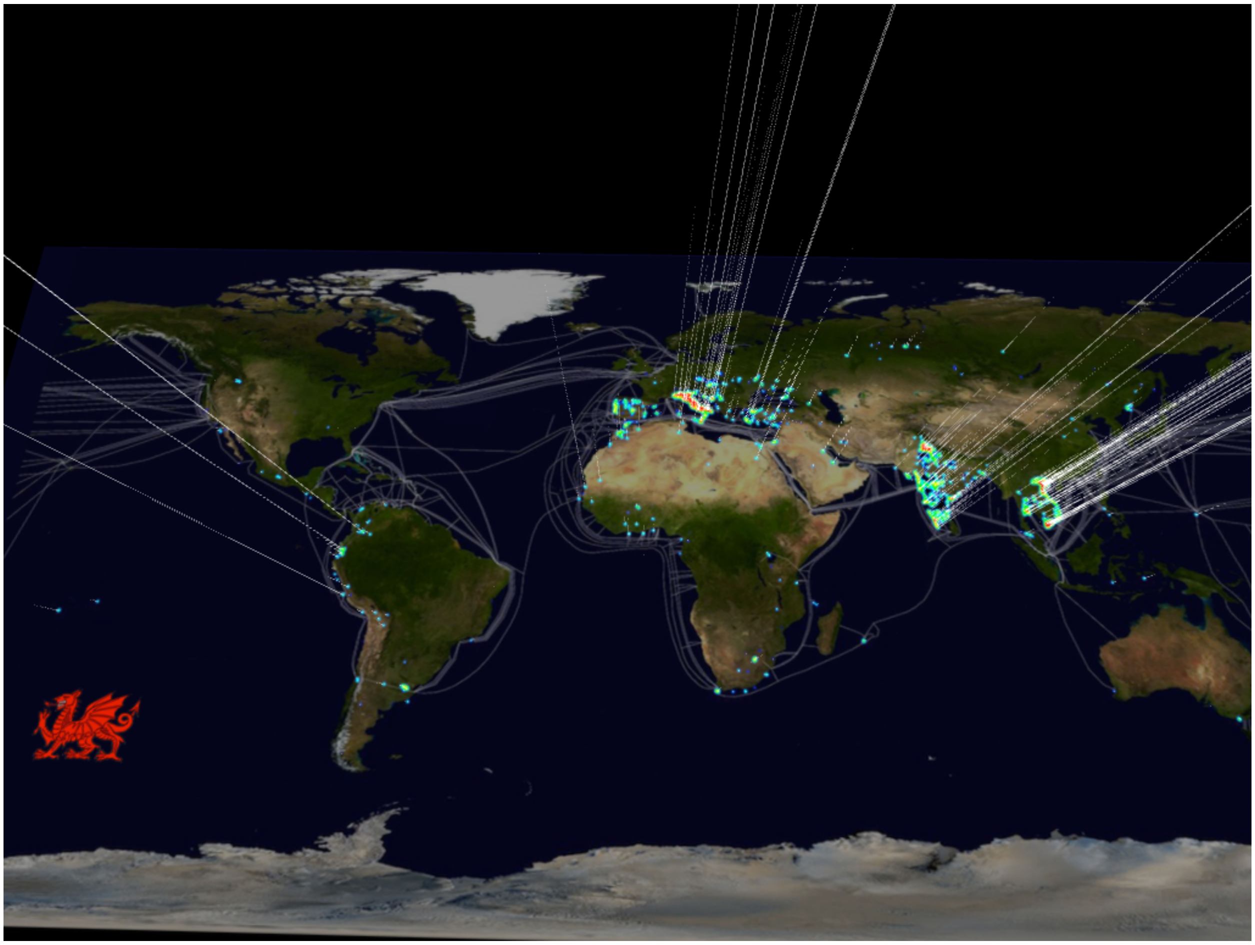
[1] See http://www.jakoblell.com/blog/2013/10/30/real-world-csrf-attack-hijacks-dns-server-configuration-of-tp-link-routers-2/ and http://rootatnasro.wordpress.com/2014/01/11/how-i-saved-your-a-from-the-zynos-rom-0-attack-full-disclosure

[2] http://niebezpiecznik.pl/post/stracil-16-000-pln-bo-mial-dziurawy-router-prawie-12-miliona-polakow-moze-byc-podatnych-na-ten-atak/

[3] https://isc.sans.edu/diary/Linksys+Worm+%22TheMoon%22+Summary%3A+What+we+know+so+far/17633

engineering standards make SOHO-type wireless routers a very attractive target for cyber criminals.

- Many cyber crime participants have become used to purchasing bots, exploit servers, and other infrastructure as managed services from other criminals. We expect that these market forces will drive advances in the exploitation of embedded systems as they have done for the exploitation of PCs.
- We have integrated victim IP addresses and other data related to SOHO pharming attacks into our no-cost community tools for network providers, as well as our commercial Threat Intelligence Feeds. For more details, visit https://www.team-cymru.org/Services/



Affected router distribution heatmap visualization

ANALYSIS

Analysis

Observed in the Wild

In January 2014, the Enterprise Intelligence Services team at Team Cymru became aware of several TP-Link Wi-Fi routers that had their DNS settings maliciously altered to send DNS requests to two new IP addresses:

```
5.45.75.11

5.45.75.36
```

The routers were both small office/home office (SOHO) class devices that provided Wi-Fi connectivity, local DNS, and DHCP services to customers, and were not using default passwords.

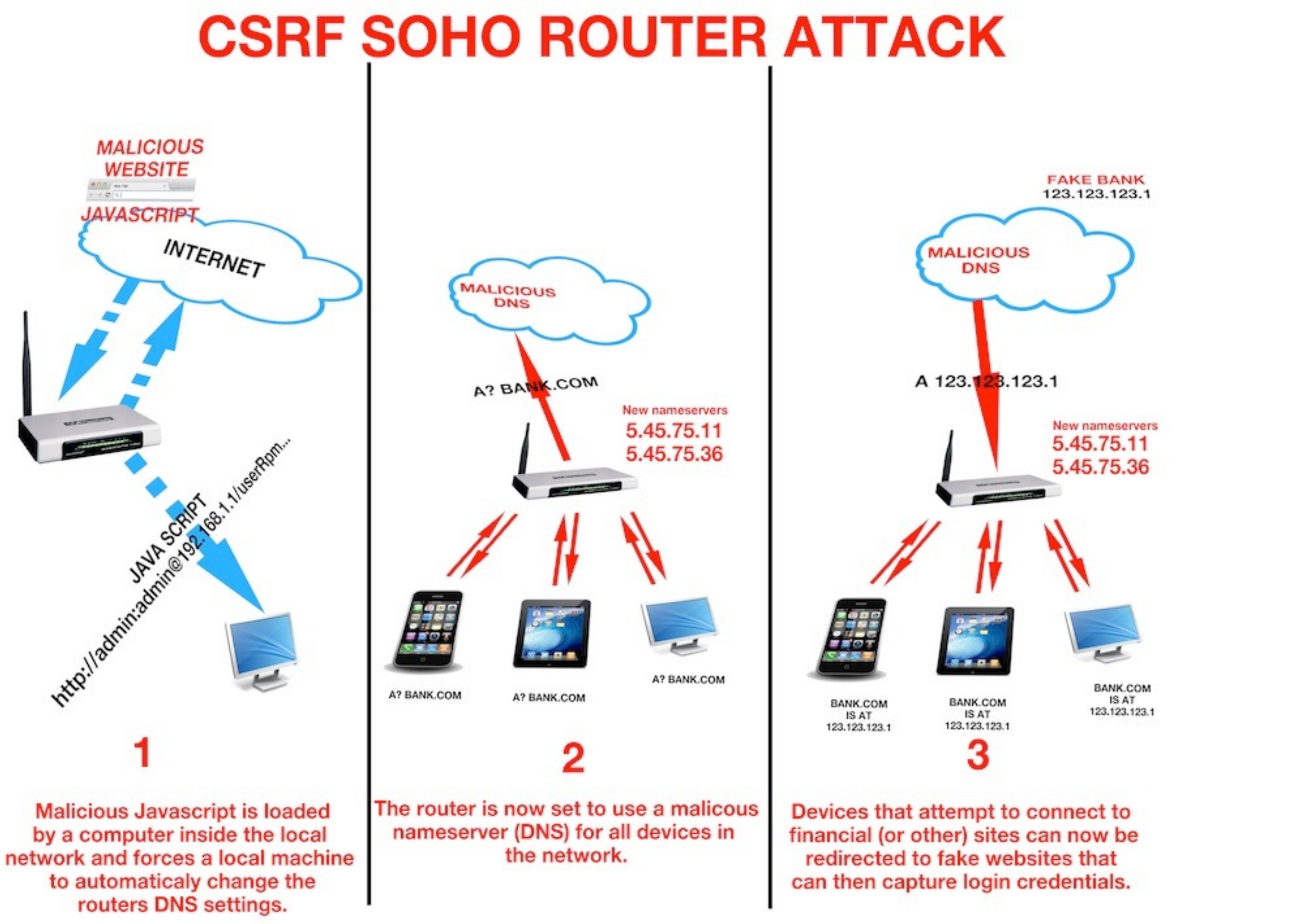

CSRF SOHO ROUTER ATTACK
MALICIOUS WEBSITE
JAVASCRIPT
INTERNET
JAVA SCRIPT
http://admin:admin@192.168.1.1/userRpm...
1
Malicious Javascript is loaded by a computer inside the local network and forces a local machine to automaticaly change the routers DNS settings.
MALICIOUS DNS
A? BANK.COM
New nameservers
5.45.75.11
5.45.75.36
A? BANK.COM
A? BANK.COM
A? BANK.COM
2
The router is now set to use a malicous nameserver (DNS) for all devices in the network.
FAKE BANK
123.123.123.1
MALICIOUS DNS
A 123.123.123.1
New nameservers
5.45.75.11
5.45.75.36
BANK.COM IS AT 123.123.123.1
BANK.COM IS AT 123.123.123.1
BANK.COM IS AT 123.123.123.1
3
Devices that attempt to connect to financial (or other) sites can now be redirected to fake websites that can then capture login credentials.

Figure 1. Three phases of SOHO router DNS exploitation via CSRF vulnerability.

However, these devices were running a firmware version vulnerable to the Cross-Site Request Forgery (CSRF) technique illustrated in Figure 1. Additionally, at least one of these models was running a version of ZyXEL ZynOS firmware recently exposed as having a serious flaw that allows attackers to download the saved configuration file, and thus the administrative credentials, from an unauthenticated URL in the web interface.[4]

Analysis of these malicious DNS servers revealed a wide range of compromised devices, including models from D-Link, Micronet, Tenda, TP-Link, and others. We have made efforts to contact these manufacturers, and we look forward to cooperating with them going forward. Victim routers were observed globally, with the largest infections in Vietnam, Italy, Thailand, Indonesia, Colombia, Turkey, Ukraine, Bosnia and Herzegovina, and Serbia.

The scale of this campaign is quite large. Figure 2 shows the distribution of victims by country over a one-week period. Over 300,000 unique IP addresses attempted DNS requests to the two servers. The two servers involved responded to any external DNS request and acted as open resolvers.

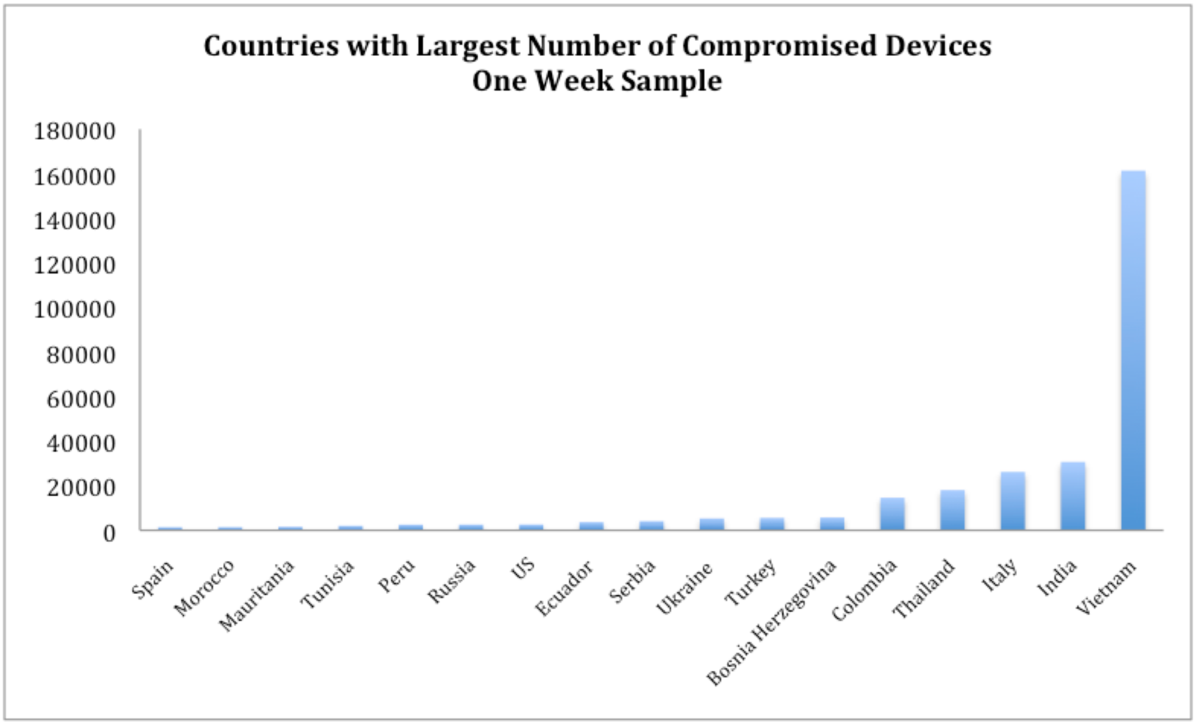


Figure 2. Victims are spread globally, likely in proportion to quantities of vulnerable devices supplied by ISPs

In our tests, the SOHO pharming DNS servers appeared to forward our DNS requests on to legitimate authoritative servers. Attempts to log into local banking websites in affected countries, and to download software updates from Adobe and others all appeared to function normally, though many requests resolved noticeably slowly or failed to complete. Websites we tested also appeared to display normal advertising using these DNS servers.

[4] http://rootatnasro.wordpress.com/2014/01/11/how-i-saved-your-a-from-the-zynos-rom-0-attack-full-disclosure

Our analysis did reveal links between the two SOHO pharming DNS servers and variety of other suspicious devices. While this may simply result from malware-related DNS activity on victim host computers, or questionable browsing activities by users behind victim SOHO devices, we continue to investigate the behavior of 5.45.75.11 and 5.45.75.36. We have also informed law enforcement about the compromised routers being set to use these servers and reached out to the provider involved, though no response has been received thus far.

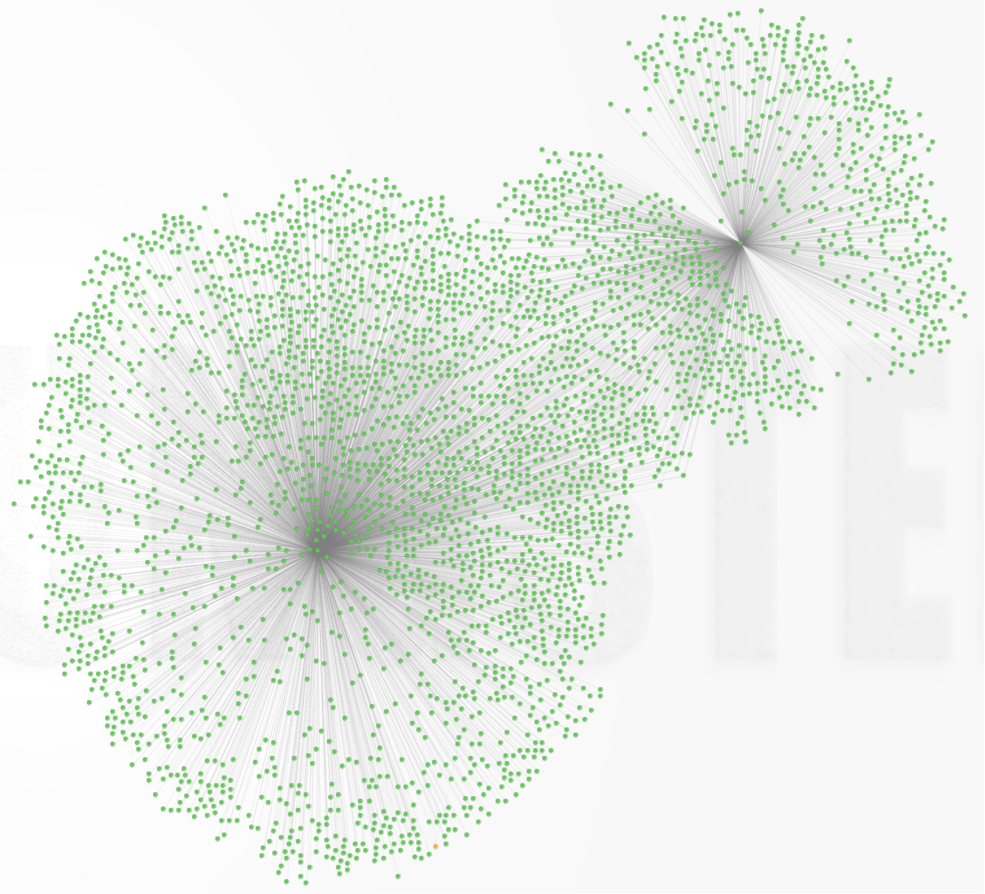


Figure 3. A sample of compromised routers linked to the malicious DNS servers

mBank: Malicious DNS Redirection Coupled with Social Engineering Attacks

What kinds of attacks are possible once a SOHO device's DNS settings have been changed? The researchers at Niebezpiecznik.pl and CERT Poland recently exposed a highly targeted attack, using DNS servers at:

95.211.241.94

95.211.205.5

In this case, the malicious DNS servers were used in a sophisticated two-stage attack against customers of the Polish mBank and other Polish retail banks.[5] The first stage involved using DNS redirection to steal credentials to individual accounts. The attackers then used these to log into victim accounts and used socially-engineered SMS messages to the victim to induce the victim to unknowingly approve a transfer of funds into the attacker's account.

Between December 2013 and February 2014, we observed approximately 80 compromised routers. Over half the victims were in Poland and most others in Russia, with small numbers in Belgium, China, Italy, the UK, and the U.S. While we believe the actual number of compromised routers is very likely higher, these numbers only reflect the devices we identified as compromised.

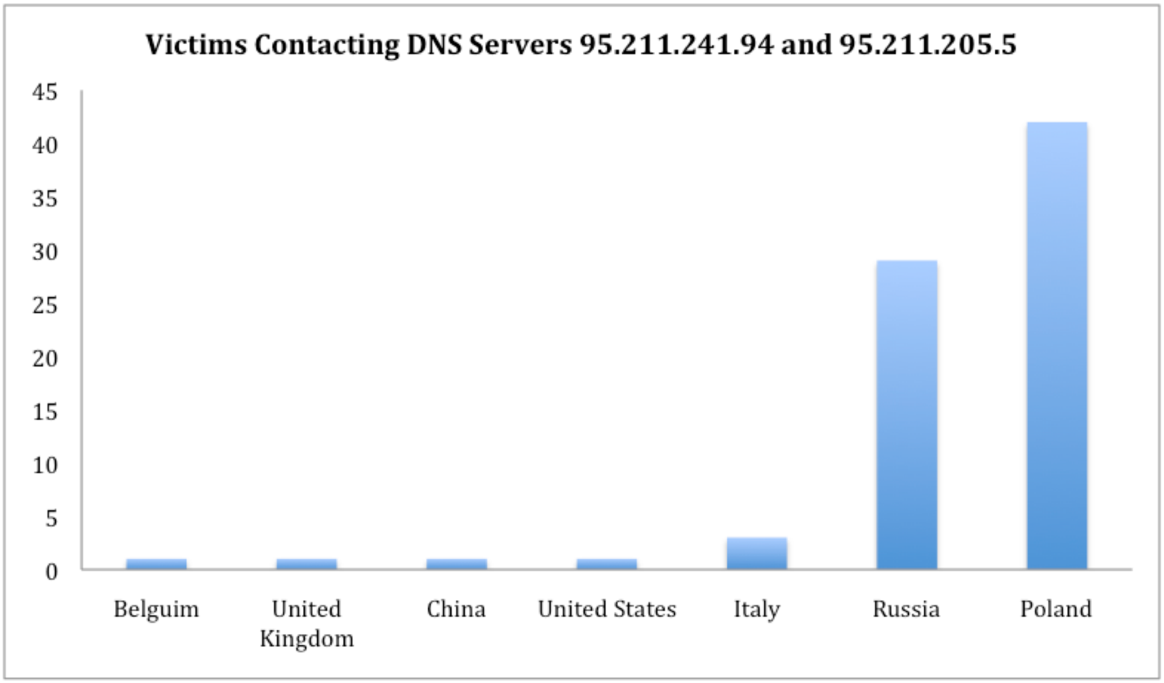


Figure 4. The DNS servers used in the mBank fraud had a small number of victims, concentrated in Poland and Russia.

Same Techniques, Different Tradecraft

While these attacks both altered the DNS server IP addresses used by victim routers, subtle differences in the tradecraft employed makes it likely that we are observing either separate campaigns by the same group, or multiple actors utilizing the same technique for different purposes.

[5] http://niebezpiecznik.pl/post/stracil-16-000-pln-bo-mial-dziurawy-router-prawie-12-miliona-polakow-moze-byc-podatnych-na-ten-atak/

In the case of the attacks against Polish banking customers, the attackers who used malicious DNS servers 95.211.241.94 and 95.211.205.5 appeared to target a small pool of users in a more concentrated geographic area and specifically focus on connections to Polish banking websites. Research by CERT Poland showed that customers of five Polish retail banks were likely targeted.[6]

These attackers appeared to have configured their malicious DNS servers to pass non-banking DNS requests solely to OpenDNS's servers for legitimate resolution.

In contrast, the attackers setting devices to the IPs 5.45.75.11 and 5.45.75.36 had compromised a very large pool of devices, and controlled large blocks of devices within specific ISPs, where the homogeneity of SOHO router models, configurations, and firmware versions likely allowed the attack to scale easily. The scale of this attack suggests a more traditional criminal intent, such as search result redirection, replacing advertisements, or installing drive-by downloads; all activities that need to be done on a large scale for profitability. The more manually-intensive bank account transfers seen in Poland would be difficult to conduct against such a large and geographically-disparate victim group.

The 5.45.75.11 and 5.45.75.36 servers also behaved differently in the way they resolved DNS queries. While the malicious servers used in the Polish banking attack funneled traffic to OpenDNS for resolution, these servers sent requests out to the authoritative servers for the domains queried and thus communicated with a far larger number of name servers.

At least one instance has been reported where crossover occurred between these two groups of IP addresses, with one device listing primary and secondary resolvers as 95.211.156.101 and 5.45.75.11, and some have suggested that this indicates the work of a single actor.[7] We were unable to determine whether this was actual evidence of overlap between different campaigns, whether one actor is behind all five IPs, or whether one campaign may have added a new DNS IP to a router previously compromised by another campaign. However, given the differences outlined above, we believe that these are separate campaigns.

Unlike earlier DNS-changing SOHO campaigns, the attacks we observed changed both primary and secondary DNS addresses to the 5.45.75.11 and 5.45.75.36 addresses mentioned earlier.[8] This risks a loss of service to ISP customers should this DNS infrastructure be shut down in the future. During our analysis we also identified that these DNS servers only responded intermittently, likely causing problems to affected users.

[6] http://www.cert.pl/news/8019/

[7] See http://security.stackexchange.com/questions/46966/dsl-modem-compromised, hxxp://in.answers.yahoo.com/question/index?qid=20140117064445AAjRi7v, and hxxp://sokosensei.wordpress.com/2014/02/06/massive-attack-on-polish-wi-fi-routers-pharming/#more-732

[8] http://www.jakoblell.com/blog/2013/10/30/real-world-csrf-attack-hijacks-dns-server-configuration-of-tp-link-routers-2/

How is it Done?

Because of the ubiquity of factory default settings on SOHO devices, some are vulnerable to simple password guessing. We observed many of the devices communicating with the suspicious DNS servers had graphical user interfaces that was accessible from the Internet, and thus vulnerable to simple brute force log-on attempts. A considerable number of the remotely accessible devices also appeared vulnerable to the "ROM-0" vulnerability published in early January.[9] This vulnerability in ZyXEL's ZynOS allows attackers to download the router's configuration file from the unauthenticated GUI URL http://[IP address]/rom-0. While the resulting ROM-0 file still has to be decompressed, this process is trivial with available tools, and automated attack scripts are available online which explicitly call out the ability to change DNS settings.[10]

In the case of the TP-Link devices we started with, these were not using default passwords, and while some models were running a vulnerable version of ZynOS, some victims were likely compromised before the ROM-0 technique was published. It is certainly possible that more than one party could have discovered the ROM-0 technique, and was exploiting this vulnerability before it became public. Another possibility is that these devices were compromised using a publicly known Cross-Site Request Forgery (CSRF) technique.[11] This technique would enable attackers to inject a null password in the device's web interface. In our examples, it worked against firmware version 3.0.0 build 120531 for the TP-Link TD-8840t, one of our initial victim systems.

```
URL used: http://192.168.1.1/Forms/tools_admin_1
```

A CSRF attack published on the 30th of October 2013 appeared to leverage stored TP-Link router login credentials in the browser to change routers DNS settings.[12] Devices vulnerable to this technique included TP-Link WR1043ND, TL-MR3020, and TL-WDR3600.

The TP-LINK CSRF URL reported in October 2013 showed the insertion of new DNS IPs:

```
http://admin:admin@192.168.1.1/userRpm/LanDhcpServerRpm.htm?
dhcpserver=1&ip1=$LOCALIP_START_RANGE&ip2=
$LOCALIP_END_RANGE&Lease=120&gateway=0.0.0.0&domain=&dnsserver=
$DNSIP&dnsserver2=$DNSIP2&Save=
```

Previous SOHO models have been vulnerable to CSRF techniques that allowed wireless WPA/WPA2 passwords to be changed, along with other malicious changes. We believe that a combination of these techniques would allow an attacker to gain control of the device and change the DNS configuration remotely.

[9] http://rootatnasro.wordpress.com/2014/01/11/how-i-saved-your-a-from-the-zynos-rom-0-attack-full-disclosure

[10] https://github.com/MrNasro/zynos-attacker

[11] See http://www.exploit-db.com/exploits/29924/ and http://cxsecurity.com/issue/WLB-2012100027 <img src="http://192.168.1.1/Forms/tools_admin_1"/>

[12] http://www.jakoblell.com/blog/2013/10/30/real-world-csrf-attack-hijacks-dns-server-configuration-of-tp-link-routers-2/

Mitigation Strategies

Organizations concerned that their customers and external partners could be victims of this type of attack should urge them to review their local router settings and security policies and contact their upstream service provider for assistance if necessary. SOHO devices should have remote user-mode administration features and GUIs disabled or, at a minimum, restricted through ACLs to only those IPs required for regular administration. Management interfaces open to the Internet create an easily detectable and exploitable vulnerability and should be disabled immediately if found.

Command line configuration of devices, where possible, is preferred to web GUI interface methods, as many of the vulnerabilities reported involve CSRF attacks against users logged into the configuration GUI. Administrators should also ensure device firmware is kept up to date.

For larger corporate networks, security professionals could also deploy HTML code to their externally facing servers to attempt to detect remote users' DNS settings, and potentially block users with compromised DNS settings, by using a html tag with a unique hostname that links visitors' DNS requests to their page visits. Note that this could add unwanted overhead for large organizations.

In the example above, the user's browser is forced to do a DNS query for a unique hostname, linking the DNS server to a unique hostname lookup. The client does a HTTP get request on this '`unique_string_detectdns.corporate-domain`' hostname and can then be identified as using malicious DNS settings. This type of DNS detection does have its limitations however, as it does not work when malicious DNS servers forward the requests to third-party services like OpenDNS.

Internal to corporate networks, these compromises are a good reminder that DNS can be abused for malware command and control and data exfiltration as well as the man-in-the-middle techniques observed here. DNS settings should be corporately controlled and potentially set at the host level as part of a secure, baseline configuration. Individual users should not have the privileges to choose their own DNS settings.

Finally, we recommend severely restricting or monitoring the deployment of SOHO Wi-Fi devices on corporate networks, and security audits should include efforts to find and remove unauthorized Wi-Fi access points, as well as scanning corporate networks for devices running SOHO services like Home Network Administration Protocol (HNAP).[13]

For end users, or those who use a SOHO device as their local DNS server, we suggest reviewing the DNS settings of local devices, and checking that the IP addresses listed belongs to your ISP's name servers. While not affected by this attack, a review of host computer DNS settings is also recommended. When in question, DNS settings can always be set to use Google's name servers (8.8.8.8 and 8.8.4.4) or those of OpenDNS (208.67.222.222 and 208.67.220.220)

[13] http://www.tenable.com/blog/hnap-protocol-vulnerabilities-pushing-the-easy-button

Conclusion

By compromising one SOHO router, an attacker can redirect traffic for every device in that network. As the compromise of mBank user accounts demonstrates, security does not stop at the host level, but extends to all devices in the network. As embedded systems begin to proliferate in both corporate and consumer networks, greater attention needs to be given to what vulnerabilities these devices introduce. Security for these devices is typically a secondary concern to cost and usability and has traditionally been overlooked by both manufacturers and consumers. As we saw in the 2012 discovery of 4 million compromised Brazilian SOHO devices, this is particularly problematic when outdated hardware is left in place or lacks ongoing support or firmware updates.[14]

With the release of the exploit code for the Moon worm available online, and the mBank campaign gaining more attention every day, we expect to see more and more malicious activity targeting SOHO devices and other embedded systems. While to date the attacks we have observed have been limited to changing user-accessible settings, Moon shows that the next likely step will be the development of tools to subvert or overwrite device firmware and give attackers better stealth and persistence on consumer devices.

Our research into this campaign did not uncover new, unknown vulnerabilities. Indeed, some of the techniques and vulnerabilities we observed have been public for well over a year. However, we still reached out to the equipment vendors affected by this campaign for their feedback and advice. We will update this paper with any recommendations and responses we receive from these vendors.

We have also notified several law enforcement agencies about the issues described in this paper, and reached out to the owners of the 5.45.75.11 and 5.45.75.36 IP addresses. Our communications to the owners of these devices, perhaps not surprisingly, went unanswered.

We are working to develop new techniques to detect these types of campaigns in the wild, and will continue to populate both our no-cost and commercial tools with this data. For more information, please visit:

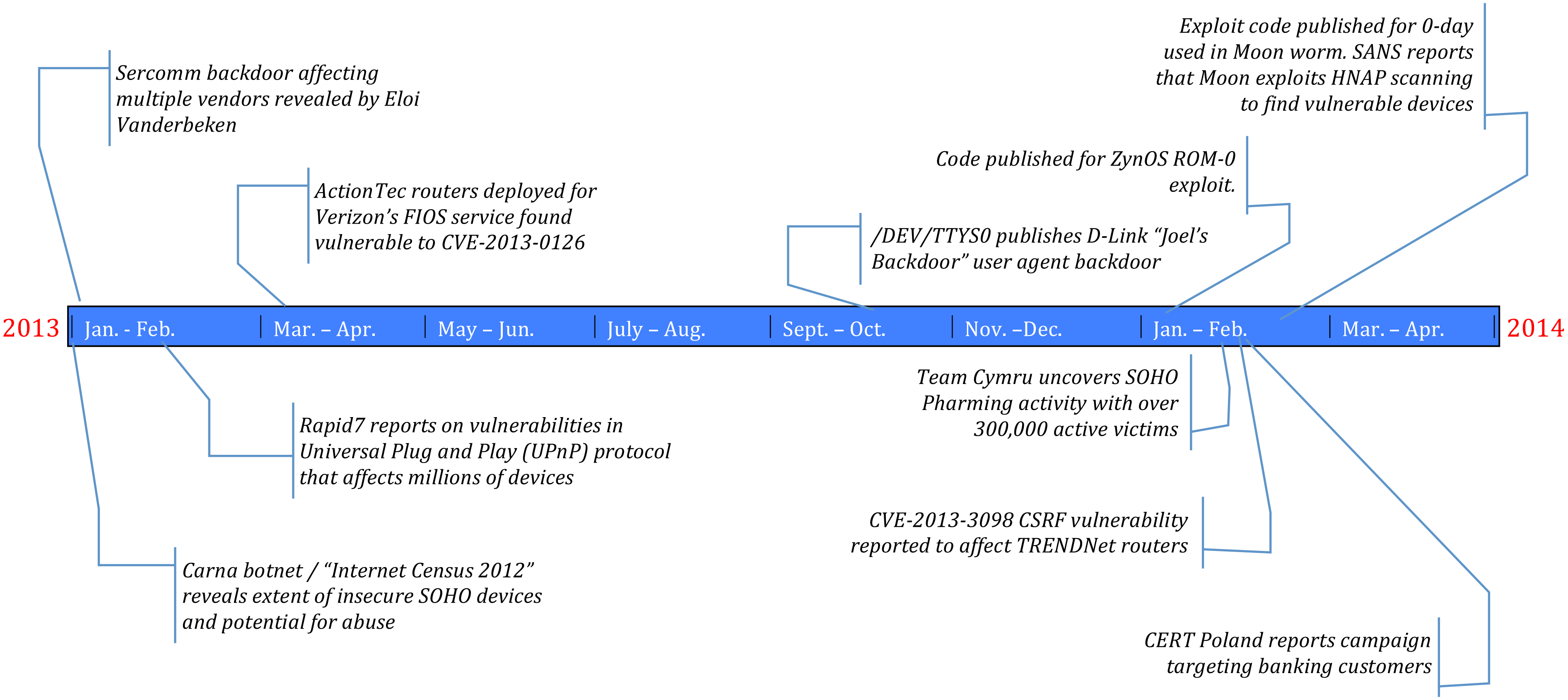
TC Console - Free: https://www.team-cymru.org/Services/TCConsole/

CSIRT Assistance Program - Free: https://www.team-cymru.org/Services/CAP/

Threat Intelligence Feeds: https://www.team-cymru.com/Services/Intel/

[14] http://www.securelist.com/en/blog/208193852/The_tale_of_one_thousand_and_one_DSL_modems

Notable SOHO Security Issues



Sercomm backdoor affecting multiple vendors revealed by Eloi Vanderbeken

Carna botnet / "Internet Census 2012" reveals extent of insecure SOHO devices and potential for abuse

Rapid7 reports on vulnerabilities in Universal Plug and Play (UPnP) protocol that affects millions of devices

ActionTec routers deployed for Verizon's FIOS service found vulnerable to CVE-2013-0126

/DEV/TTYS0 publishes D-Link "Joel's Backdoor" user agent backdoor

Code published for ZynOS ROM-0 exploit.

Team Cymru uncovers SOHO Pharming activity with over 300,000 active victims

CVE-2013-3098 CSRF vulnerability reported to affect TRENDNet routers

CERT Poland reports campaign targeting banking customers

Exploit code published for 0-day used in Moon worm. SANS reports that Moon exploits HNAP scanning to find vulnerable devices