Akamai Security Intelligence & Threat Research

SUBSCRIBE

Latest

UPNPROXY: ETERNALSILENCE

By Akamai SIRT Alerts **November 28, 2018 9:24 AM**

0 Comments

By, Chad Seaman

OVERVIEW:

UPnProxy is alive and well. There are 277,000 devices, out of a pool of 3.5 million, running vulnerable implementations of UPnP. Of those, Akamai can confirm that more than 45,000 have been compromised in a widely distributed UPnP NAT injection campaign. These injections expose machines living behind the router to the Internet and appear to target the service ports used by SMB.

BACKGROUND:

Earlier this year, Akamai researchers reported on how Universal Plug and Play (UPnP) was being abused by attackers to conceal traffic, creating a malicious proxy system we've called UPnProxy. Because UPnProxy can be leveraged to route an attacker's traffic at will, there is a serious risk that this flaw can be leveraged in a number of attacks, including spam, phishing, click fraud, and DDoS.

Now, six months later, we're seeing evidence that UPnProxy alive and well. Out of a potential victim pool of 3.5 million vulnerable devices, 277,000 of them are vulnerable to UPnProxy. Our scanning revealed at least 45,000 actively injected machines, those with the telltale routes already in their port hile some of the campaigns observed in the original research have since disappeared, a new campaign of injections has been discovered.

In Akamai's previous research, we highlighted the possibility that attackers could leverage UPnProxy to exploit systems living behind the compromised router. Unfortunately, data from this recent batch of injections suggests this is exactly what's happening.

For home users, these attacks can lead to a number of complications, such as degraded service, malware infections, ransomware, and fraud. But for business users, these recent developments could mean systems that were never supposed to exist on the internet in the first place, could now be living there unknowingly, greatly increasing their chances of being compromised. Even more concerning, the services being exposed by this particular campaign have a history of exploitation related to crippling worms and ransomware campaigns targeting both Windows and Linux platforms.

ETERNALSILENCE:

On November 7, while working on a project related to the original UPnProxy discoveries, researchers at Akamai discovered a new family of injections, which they've dubbed Eternal Silence. The name EternalSilence comes from port mapping descriptions left by the attackers. In addition, these new attacks are believed to be leveraging the Eternal family of exploits.

Normally, the NewPortMappingDescription field on the routers would state something like 'Skype' for legitimate injections, in UPnProxy campaigns this field is also attacker controlled. The new rulesets discovered by Akamai - affecting over 45,000 routers - all contain 'galleta silenciosa' or 'silent cookie/cracker' in Spanish. These sets of injections attempt to expose the TCP ports 139 and 445 on devices behind the router.

```
{"NewProtocol": "TCP", "NewInternalPort": "445", "NewInternalClient": "192.168.10.212",

"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "47669"}
```

Figure 1: An example EternalSilence injections found in the wild

Taking current disclosures and events into account, Akamai researchers believe that someone is attempting to compromise millions of machines living behind the vulnerable routers by leveraging the EternalBlue and EternalRed exploits.

only see the injections themselves and not the final payloads that would be directed at the machines exposed. However, a successful attack could yield a target rich environment, opening up the chance for such things as ransomware attacks, or a persistent foothold on the network.

Currently, the 45,113 routers with confirmed injections expose a total of 1.7 million unique machines to the attackers. We've reached this conclusion by logging the number of unique IPs exposed per router, and then added them up. It is difficult to tell if these attempts led to a successful exposure as we don't know if a machine was assigned that IP at the time of the injection. Additionally, there is no way to tell if EternalBlue or EternalRed was used to successfully compromise the exposed machine. However, if only a fraction of the potentially exposed systems were successfully compromised and fell into the hands of the attackers, the situation would quickly turn from bad to worse.

The Attacks:

After observing millions of successful injections attempting to expose millions of machines running SMB services, Akamai researchers speculate the actors behind EternalSilence are running this campaign with the intention of leveraging the Eternal family of exploits.

EternalBlue (CVE-2017-0144): The widely-known exploit stolen from the NSA and released by Shadow Brokers, impacts every version of Windows, and even after widespread patching took place (MS17-010), criminals still managed to leverage the exploit code to launch devastating attacks, such as WannaCry and NotPetya.

EternalRed (CVE-2017-7494): Sometimes known as the sibling to EternalBlue; targets Samba and opens the Eternal family up to Linux-based systems. It's been used in a number of crypto-mining campaigns and became widely-known as SambaCry.

Recent scans suggest that these attackers are being opportunistic. One possibility is that they're scanning the entire internet for SSDP and pivoting to the TCP UPnP daemons. Alternatively,based on scan results and banner grabs, they're targeting a set of devices which utilize static ports (TCP/2048) and paths (/etc/linuxigd/gatedesc.xml) for their UPnP daemons.

They're doing this in order to blindly inject SMB port forwards. This is only possible because there are millions (3.5 million) of vulnerable routers on the internet, and plenty of them (277,000) are running vulnerable implementations of UPnP that expose themselves and their IGD (Internet Gateway

The goal here isn't a targeted attack. It's an attempt at leveraging tried and true off the shelf exploits, casting a wide net into a relatively small pond, in the hopes of scooping up a pool of previously inaccessible devices.

This shotgun approach may be working too, because there is a decent possibility that machines unaffected by the first round of EternalBlue and EternalRed attacks (that may have remained unpatched) were safe only because they weren't exposed directly to the internet. They were in a relatively safe harbor living behind the NAT.

The EternalSilence attacks remove this implied protection granted by the NAT from the equation entirely, possibly exposing a whole new set of victims to the same old exploits.

```
{"NewProtocol": "TCP", "NewInternalPort": "445", "NewInternalClient": "192.168.10.165",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "47622"},
{"NewProtocol": "TCP", "NewInternalPort": "139", "NewInternalClient": "192.168.10.166",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "28823"},
{"NewProtocol": "TCP", "NewInternalPort": "445", "NewInternalClient": "192.168.10.166",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "47623"},
{"NewProtocol": "TCP", "NewInternalPort": "139", "NewInternalClient": "192.168.10.183",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "28840"},
{"NewProtocol": "TCP", "NewInternalPort": "139", "NewInternalClient": "192.168.10.194",
 "NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "28851"},
{"NewProtocol": "TCP", "NewInternalPort": "139", "NewInternalClient": "192.168.10.198",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "28855"},
{"NewProtocol": "TCP", "NewInternalPort": "139", "NewInternalClient": "192.168.10.207",
 "NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "28864"},
{"NewProtocol": "TCP", "NewInternalPort": "139", "NewInternalClient": "192.168.10.209",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "28866"},
{"NewProtocol": "TCP", "NewInternalPort": "139", "NewInternalClient": "192.168.10.212",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "28869"},
{"NewProtocol": "TCP", "NewInternalPort": "445", "NewInternalClient": "192.168.10.212",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "47669"}
```

Figure 2: A larger sample of EternalSilence injections found on a single router

Lacking Visibility:

bility into them on an injected router. The UPnP protocol itself is designed to let machines automagically request NAT/port forwarding capabilities from the Internet Gateway Device (IGD) operated by the router. Inspecting these rules requires the use of UPnP tool sets, device scanning, and manual rule inspection to achieve some level of detection.

The best way to identify if a device is vulnerable or actively being leveraged for UPnProxying is to scan an end-point and audit it's NAT table entries. There are a handful of frameworks and libraries available in multiple languages to aid in this process. Below is a simple bash script used during this research. It is capable of testing a suspected vulnerable endpoint by attempting to dump the first 10,000 UPnP NAT entries from the devices exposed TCP daemon.

```
#!/usr/bin/bash url=$1 soap_head='<?xml version="1.0" encoding="utf-8"?>
<s:Envelope s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" xmlns:s="http://s

<s:Body>


<u:GetGenericPortMappingEntry xmlns:u="urn:upnp-org:serviceId:WANIPConnection.1#GetGener
<NewPortMappingIndex>'
soap_tail='</NewPortMappingIndex></u:GetGenericPortMappingEntry></s:Body></s:Envelope>'



for i in `seq 1 10000`; do


    payload=$soap_head$i$soap_tail


    curl -H 'Content-Type: "text/xml;charset=UTF-8"' -H 'SOAPACTION:
"urn:schemas-upnp-org:service:WANIPConnection:1#GetGenericPortMappingEntry"' --data "$pa
"done
```

Figure 3: Bash script to dump UPnP NAT entries

```
<?xml version="1.0"?>


<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://
<u:GetGenericPortMappingEntryResponse xmlns:u="urn:schemas-upnp-org:service:WANIPConnect
<NewRemoteHost></NewRemoteHost><NewExternalPort>50694</NewExternalPort>
<NewProtocol>TCP</NewProtocol><NewInternalPort>53</NewInternalPort><NewInternalClient>8.8
<NewEnabled>1</NewEnabled><NewPortMappingDescription>node:nat:upnp</NewPortMappingDescri
</u:GetGenericPortMappingEntryResponse></s:Body></s:Envelope>

<?xml version="1.0"?>


<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://
<u:GetGenericPortMappingEntryResponse xmlns:u="urn:schemas-upnp-org:service:WANIPConnect
<NewExternalPort>30932</NewExternalPort><NewProtocol>TCP</NewProtocol><NewInternalPort>5
<NewInternalClient>8.8.8.8</NewInternalClient><NewEnabled>1</NewEnabled><NewPortMappingD
<NewLeaseDuration>0</NewLeaseDuration></u:GetGenericPortMappingEntryResponse></s:Body></


...snip...
```

Figure 4: Results from a UPnProxy injected host

Impact:

Victims of this attack will be at the mercy of the attackers, because they'll have machines existing on the internet that were previously segmented, and they'll have no idea this is happening. Moreover, machines within the network that had a low priority when it came to patches will become easy pickings.

Mitigations:

In order to recover from or prevent an attack, device owners can either purchase a new router that doesn't have the UPnP vulnerabilities that enable this type of abuse or ensure that UPnP is disabled if they're vulnerable.

the router itself or possibly flashing the router to the original factory settings and configure it with UPnP completely disabled. It's also advisable to check for firmware updates, as some routers may have published fixes for this issue.

There is a possibility that machines within the network that were exposed may have already been compromised, and if that's the case, cleaning the router isn't going to be enough. So it's wise to check for odd traffic on the LAN side, especially if the machine is running vulnerable versions of Windows or Linux that could be compromised by EternalBlue or EternalRed.

CLOSING:

Criminals are clever, and will take any advantage they can get when it comes to exploiting systems and services. So, while it is unfortunate to see UPnProxy being actively leveraged to attack systems previously shielded behind the NAT, it was bound to happen eventually. That these attacks likely leverage two well-known vulnerabilities, which have been patched for some time, should come as no surprise.

Asset management isn't easy, and because some assets have a lower rotation rate or a lower patch rate, the criminals leveraging EternalSilence are looking to gain access to critical systems deemed an acceptable risk to some organizations. Sometimes these systems are overlooked because of the adage of 'if it ain't broke, don't fix it', a stance that has come to haunt many organizations over the years.

Administrators looking to try and gain an edge can scan themselves and see if they're exposed to these vulnerabilities, including scanning their UPnP NAT table to look for oddities. Lastly, perhaps investments into new routers and ensuring their configuration disables UPnP is a better long-term solution.

Leave a comment

Name*

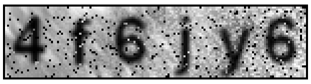
Email Address*

URL

□ Remember personal info?

Comments* (You may use HTML tags for style)

Captcha*:



Type the characters you see in the picture above.

Preview Submit

Authors

We're Social