Microsoft Exchange servers are getting hacked via ProxyShell exploits

Lawrence Abrams

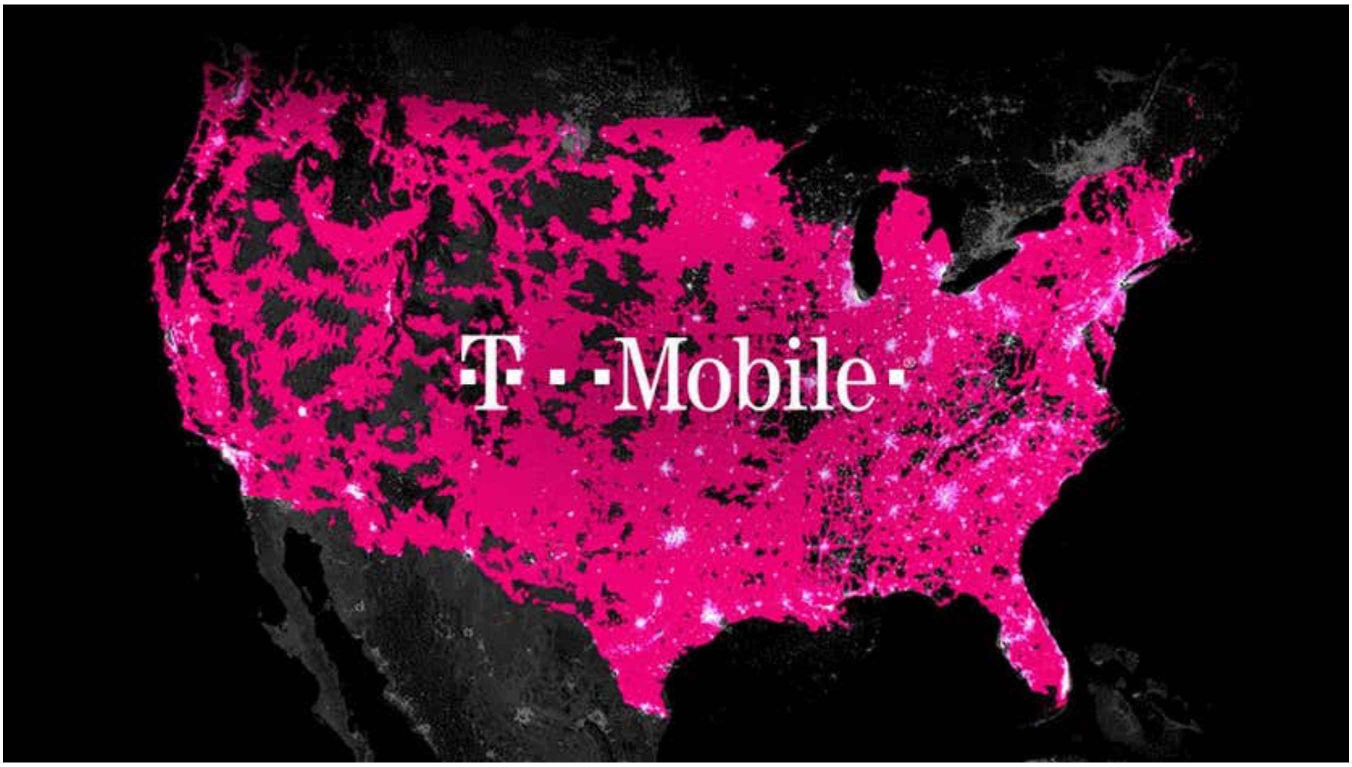
Threat actors are actively exploiting Microsoft Exchange servers using the ProxyShell vulnerability to install backdoors for later access.

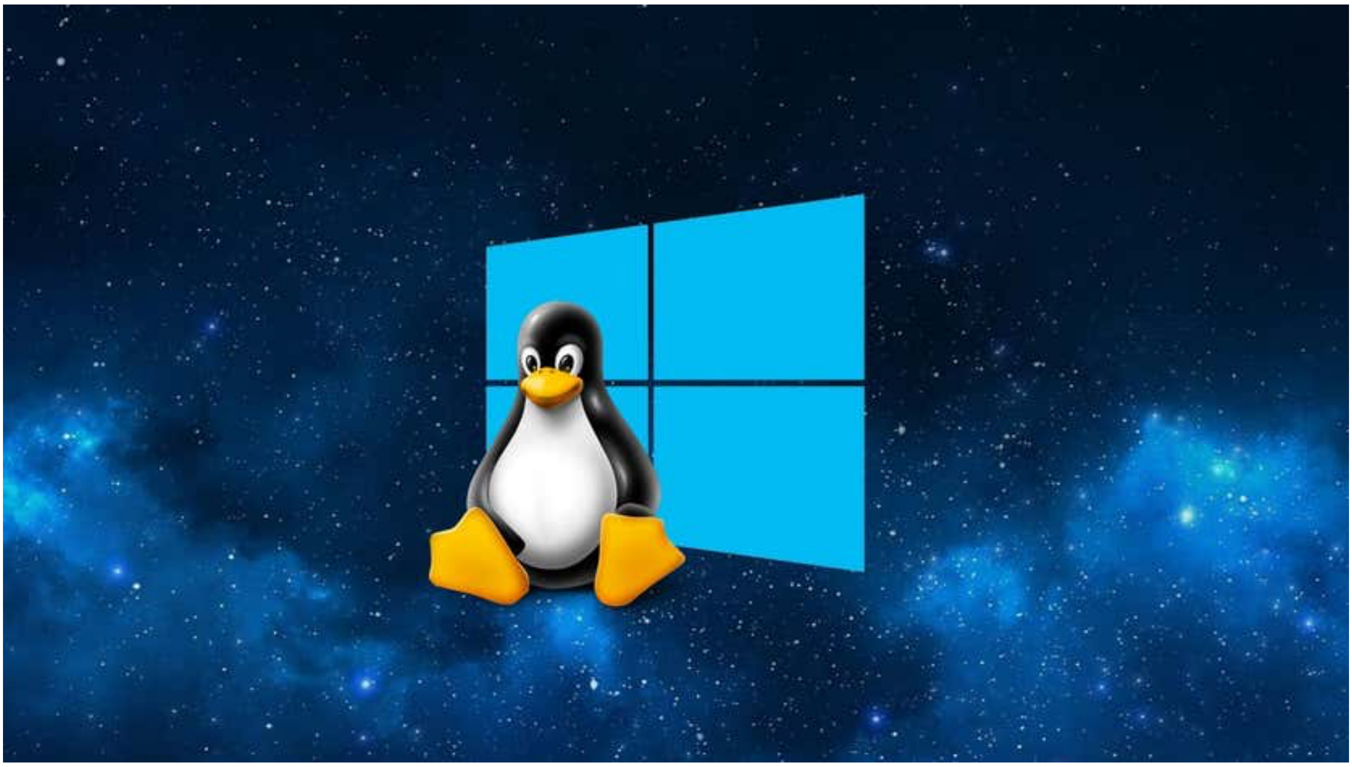
ProxyShell is the name of an attack that uses three chained Microsoft Exchange vulnerabilities to perform unauthenticated, remote code execution.

The three vulnerabilities, listed below, were discovered by Devcore Principal Security Researcher Orange Tsai, who chained them together to take over a Microsoft Exchange server in April's Pwn2Own 2021 hacking contest.

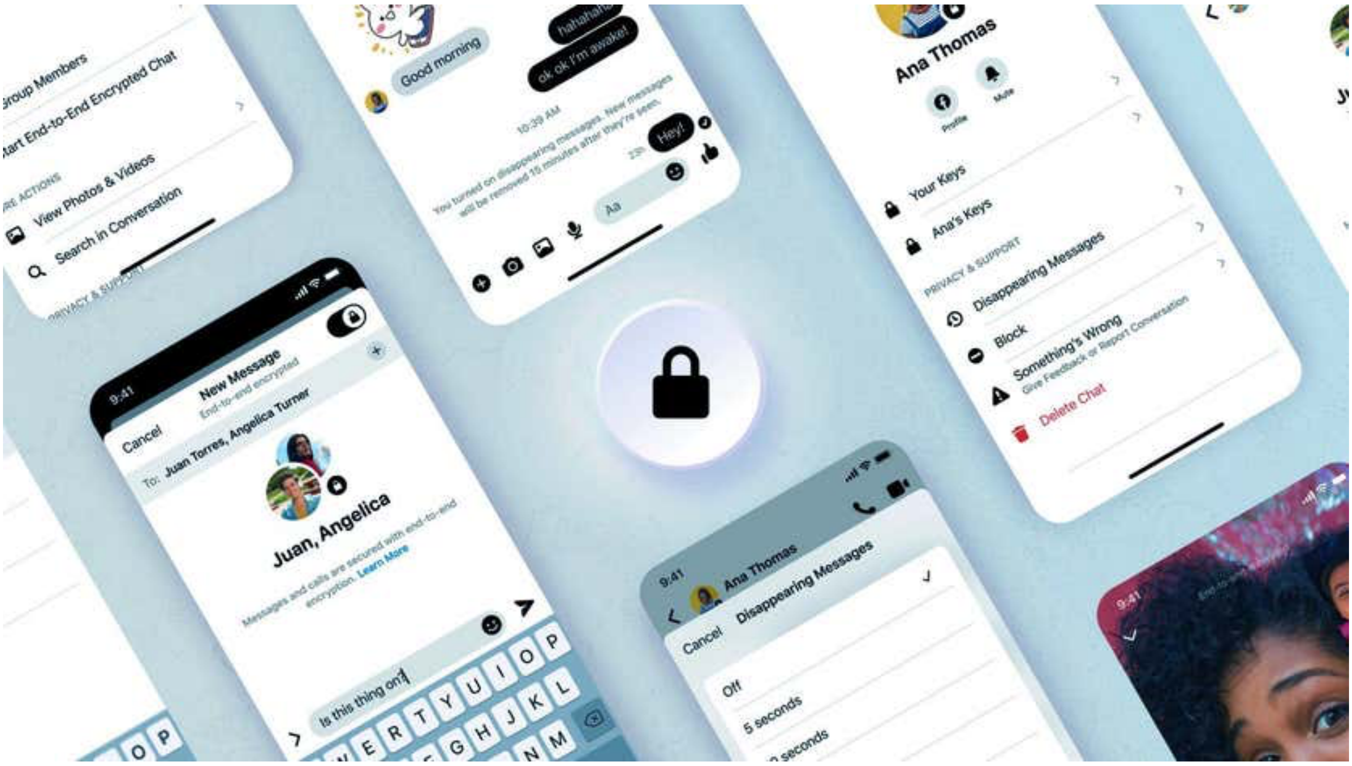
bleepingcomputer
From a bleeping computer to a working computer

Top Articles





[Read More](https://www.bleepingcomputer.com)



US brokers warned of ongoing phishing attacksimpersonating FINRA

- CVE-2021-34473 - Pre-auth Path Confusion leads to ACL Bypass *(Patched in April by KB5001779)*
- CVE-2021-34523 - Elevation of Privilege on Exchange PowerShell

Backend *(Patched in April by KB5001779)*
- CVE-2021-31207 - Post-auth Arbitrary-File-Write leads to RCE *(Patched in May by KB5003435)*

Last week, Orange Tsai gave a Black Hat talk about recent Microsoft Exchange vulnerabilities he discovered when targeting the Microsoft Exchange Client Access Service (CAS) attack surface.

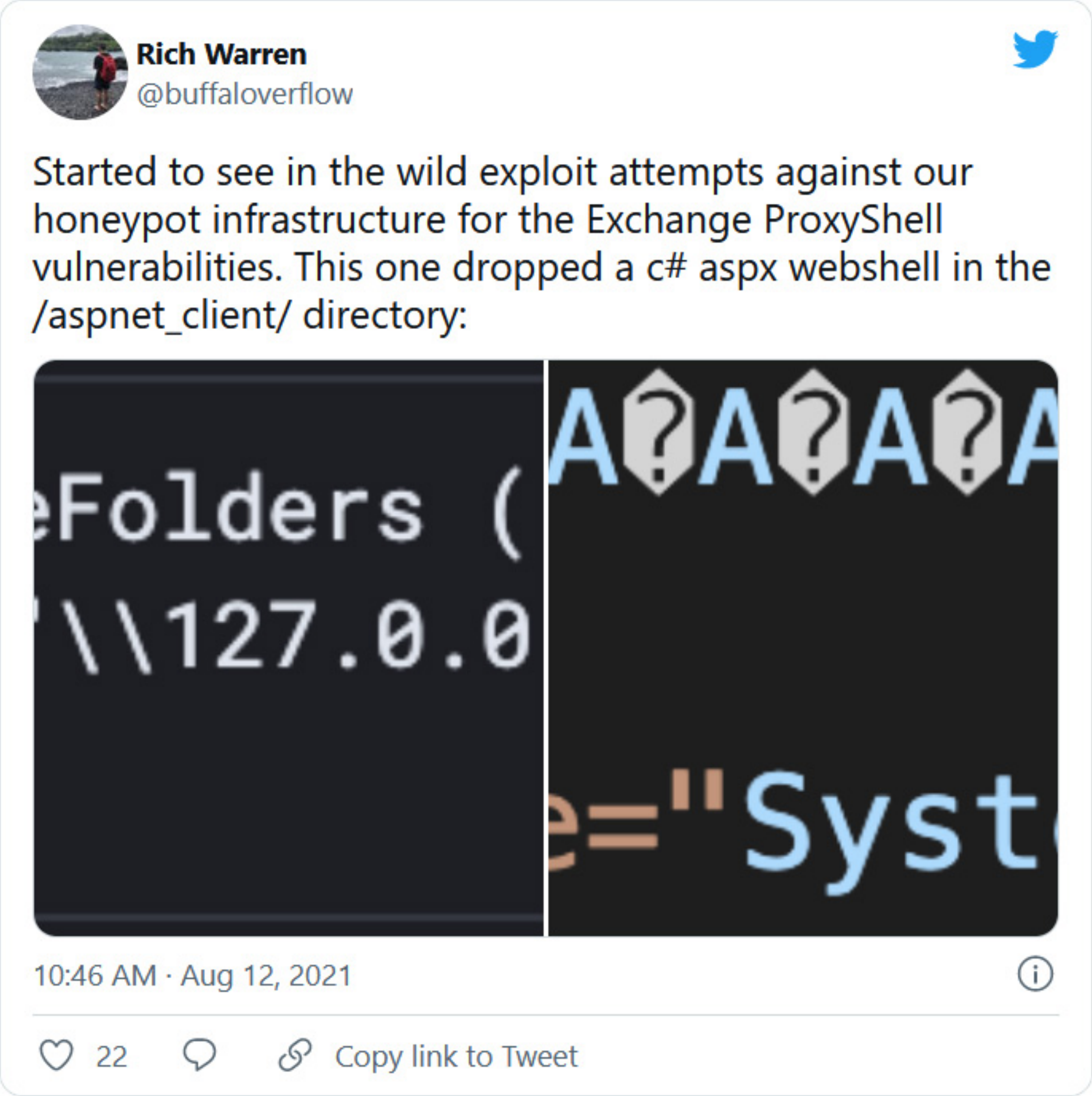
Tsai revealed that the ProxyShell exploit uses Microsoft Exchange's AutoDiscover feature to perform an SSRF attack as part of the talk.

After watching the talk, security researchers PeterJson and Nguyen Jang published more detailed technical information about successfully reproducing the ProxyShell exploit.

Soon after, security researcher Kevin Beaumont began seeing threat actors scan for Microsoft Exchange servers vulnerable to ProxyShell.

ProxyShell actively exploited to drop webshells

Today, Beaumont and NCC Group's vulnerability researcher Rich Warren disclosed that threat actors have exploited their Microsoft Exchange honeypots using the ProxyShell vulnerability.



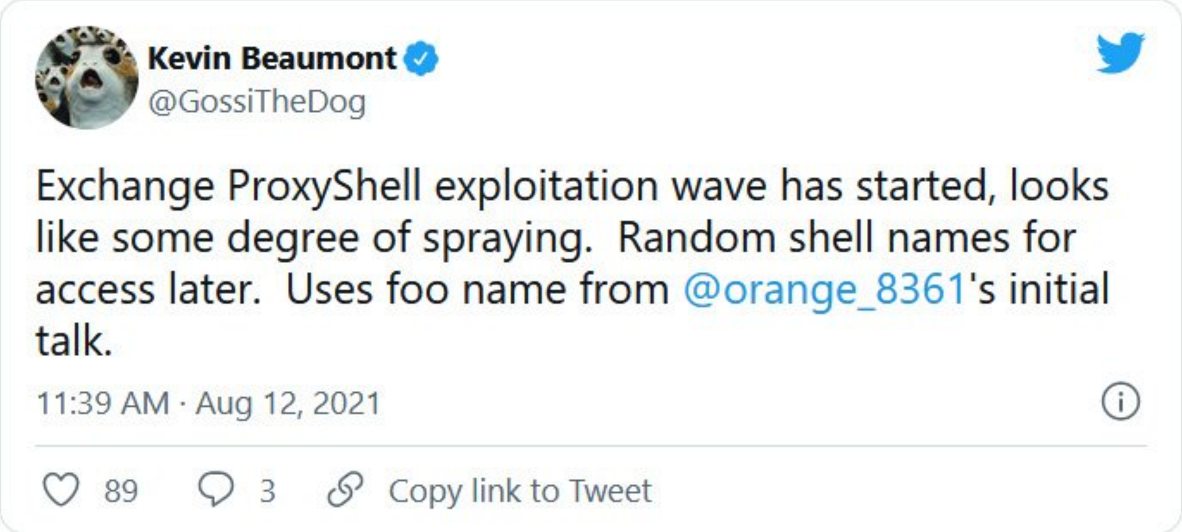
Rich Warren
@buffaloverflow

Started to see in the wild exploit attempts against our honeypot infrastructure for the Exchange ProxyShell vulnerabilities. This one dropped a c# aspx webshell in the /aspnet_client/ directory:

```
eFolders (
'\\127.0.0
```

```
A?A?A?A
e="Syst
```

10:46 AM · Aug 12, 2021



Kevin Beaumont
@GossiTheDog

Exchange ProxyShell exploitation wave has started, looks like some degree of spraying. Random shell names for access later. Uses foo name from @orange_8361's initial talk.

11:39 AM · Aug 12, 2021

When exploiting Microsoft Exchange, the attackers are using an initial URL like:

```
https://Exchange-server/autodiscover/autodiscover.json?@foo.com/mapi/nspi/?
```

Note: The email address listed in the URL does not have to exist and change between attackers.

The exploit is currently dropping a webshell that is 265KB in size to the 'c:\inetpub\wwwroot\aspnet_client\' folder.

Last week, Jang explained to BleepingComputer that 265KB is the minimum files size that can be created using the ProxyShell exploit due to its abuse of the Mailbox Export function of Exchange Powershell to create PST files.

From a sample shared by Warren with BleepingComputer, the webshells consist of a simple authentication-protected script that the threat actors can use to upload files to the compromised Microsoft Exchange server.

Warren said the threat actors use the first webshell to upload an additional webshell to a remotely accessible folder and two executables to the C:\Windows\System32 folders, listed below:

```
C:\Windows\System32\createhidetask.exe
C:\Windows\System32\ApplicationUpdate.exe
```

If the two executables can't be found, another webshell will be created in the following folder as random-named ASPX files.

```
C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\
```

The attackers use the second webshell to launch the 'createhidetask.exe,' which creates a scheduled task named 'PowerManager' that launches the 'ApplicationUpdate.exe' executable at 1 AM every day.

Warren told BleepingComputer that the ApplicationUpdate.exe executable is a custom .NET loader used as a backdoor.

"ApplicationUpdate.exe is the .NET loader which fetches another .NET binary from a remote server (which is currently serving a benign payload)," explained Warren.

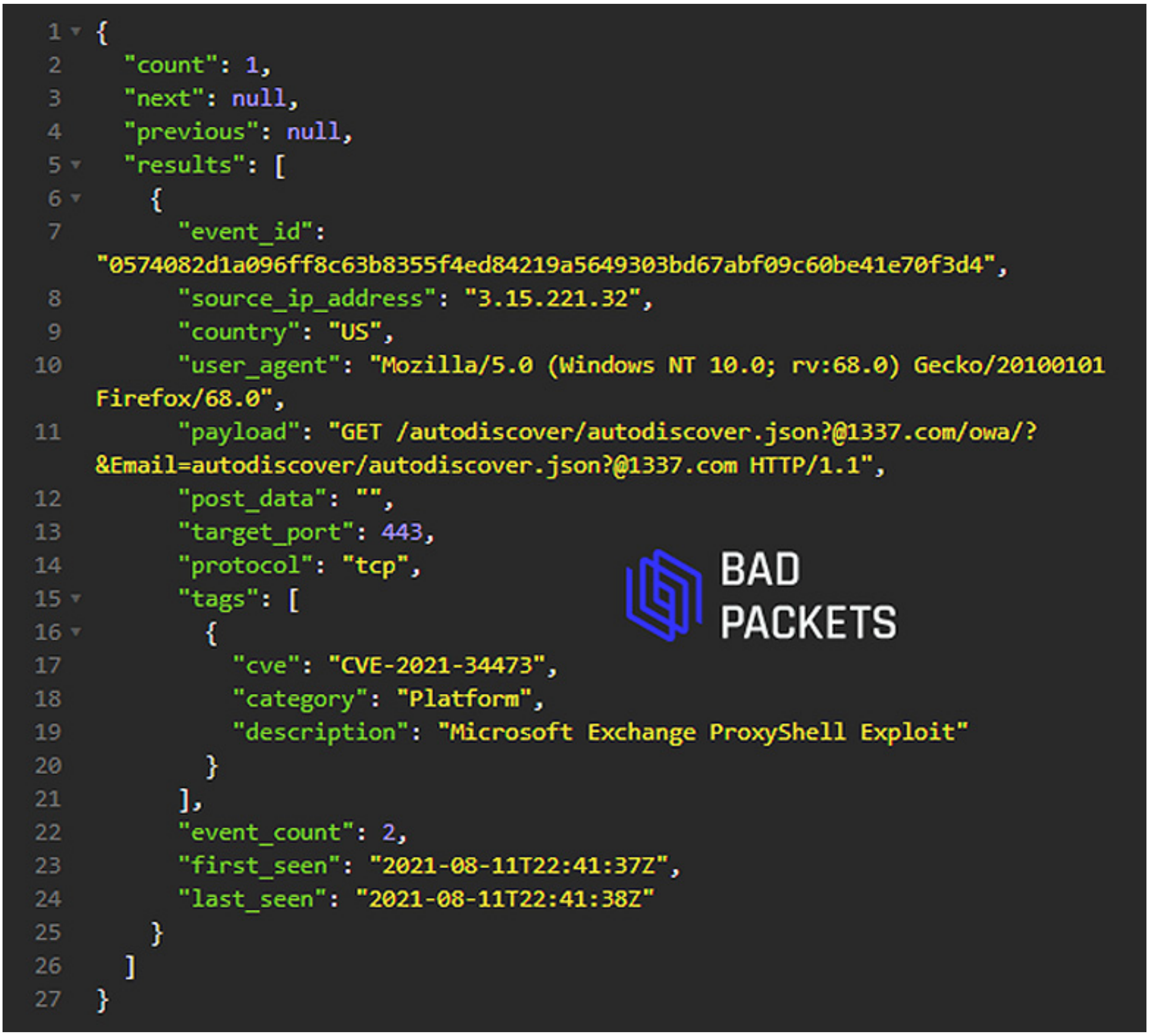
While the current payload is benign, it is expected to be swapped out with a malicious payload once enough servers are compromised.

Cybersecurity intelligence firm Bad Packets told BleepingComputer that they currently see threat actors scan for vulnerable ProxyShell devices from IP addresses in the USA, Iran, and the Netherlands.

The known addresses are:

- 3.15.221.32
- 194.147.142.0/24

BadPackets also said that the email domains used in the scans have been from @abc.com and @1337.com, as shown below.



```
{
  "count": 1,
  "next": null,
  "previous": null,
  "results": [
    {
      "event_id": "0574082d1a096ff8c63b8355f4ed84219a5649303bd67abf09c60be41e70f3d4",
      "source_ip_address": "3.15.221.32",
      "country": "US",
      "user_agent": "Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0",
      "payload": "GET /autodiscover/autodiscover.json?@1337.com/owa/?&Email=autodiscover/autodiscover.json?@1337.com HTTP/1.1",
      "post_data": "",
      "target_port": 443,
      "protocol": "tcp",
      "tags": [
        {
          "cve": "CVE-2021-34473",
          "category": "Platform",
          "description": "Microsoft Exchange ProxyShell Exploit"
        }
      ],
      "event_count": 2,
      "first_seen": "2021-08-11T22:41:37Z",
      "last_seen": "2021-08-11T22:41:38Z"
    }
  ]
}
```

Bad Packets detecting a ProxyShell scan

Now that threat actors are actively exploiting vulnerable Microsoft Exchange servers, Beaumont advises admins to perform Azure Sentinel queries to check if their devices have been scanned.

```
W3CIISLog
| where csUriStem == "/autodiscover/autodiscover.json"
| where csUriQuery has "PowerShell" | where csMethod == "POST"
```

For those who have not updated their Microsoft Exchange server recently, it is strongly recommended to do so immediately.

As the previous ProxyLogon attacks led to ransomware, malware, and data theft on exposed servers, we will likely see similar attacks using ProxyShell.

Related Articles:

Microsoft Exchange servers scanned for ProxyShell vulnerability, Patch Now

Microsoft fixes Windows Print Spooler PrintNightmare vulnerability

Microsoft August 2021 Patch Tuesday fixes 3 zero-days, 44 flaws

Microsoft's incomplete PrintNightmare patch fails to fix vulnerability

Actively exploited bug bypasses authentication on millions of routers