Threat Spotlight: New InterPlanetary Storm variant targeting IoT devices

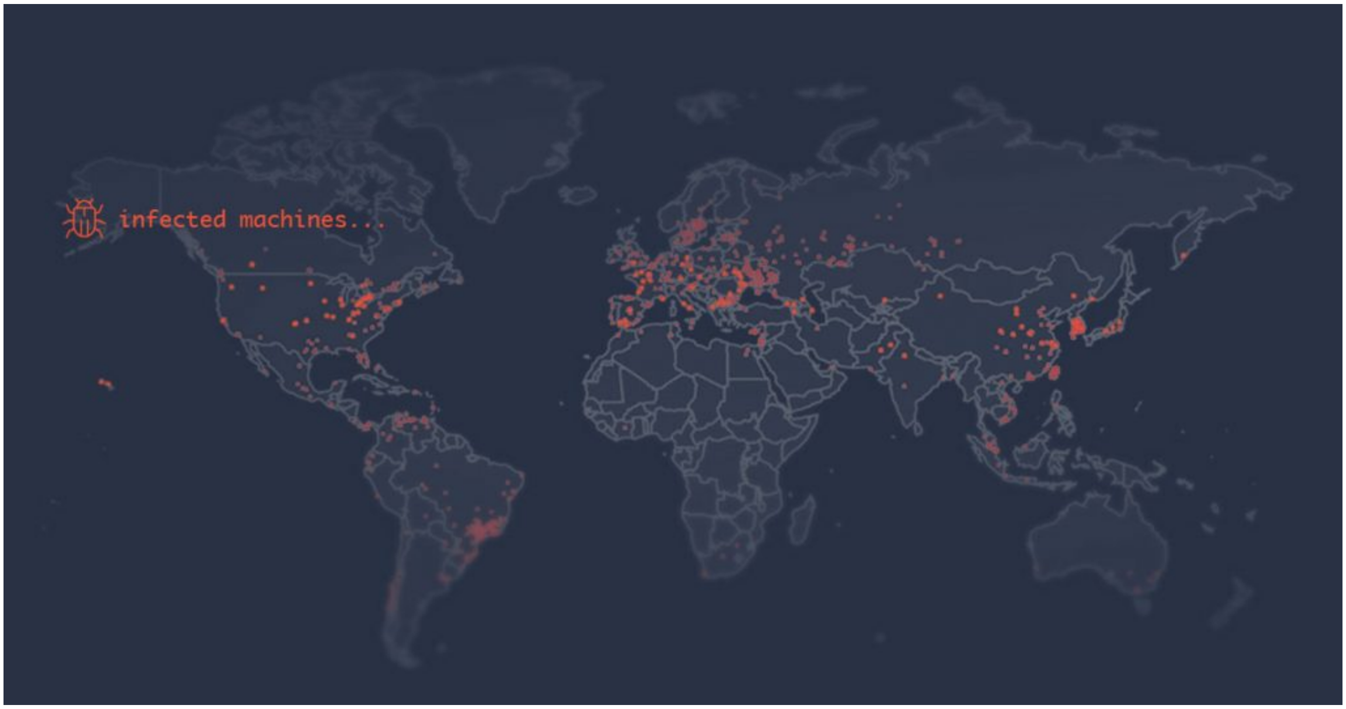
October 1, 2020

The cybercriminal organization behind the InterPlanetary Storm malware has released a new variant into the wild, now targeting Mac and Android devices in addition to Windows and Linux machines. The malware is building a botnet, which Barracuda researchers estimate currently includes roughly 13,500 infected machines located in 84 different countries around the world, and that number continues to grow.

The majority of the machines infected by the malware are located in Asia.

- 59% of infected machines are in Hong Kong, South Korea, and Taiwan
- 8% are in Russia and Ukraine
- 6% are in Brazil
- 5% are in the United States and Canada
- 3% are in Sweden
- 3% are in China
- All other countries are 1% or less

Here is a closer look at this evolving threat and solutions to help detect, block, and remediate the attacks.



Highlighted Threat

New variant of InterPlanetary Storm malware — This new malware variant gains access to machines by running a dictionary attack against SSH servers, similar to FritzFrog, another peer-to-peer (p2p) malware. It can also gain entry by accessing open ADB (Android Debug Bridge) servers. The malware detects the CPU architecture and running OS of its victims, and it can run on ARM-based machines, an architecture that is quite common with routers and other IoT devices.

The malware is called InterPlanetary Storm because it uses the InterPlanetary File System (IPFS) p2p network and its underlying libp2p implementation. This allows infected nodes to communicate with each other directly or through other nodes (i.e. relays).

The first variant of Interplanetary Storm, which targeted Windows machines, was uncovered by researchers at Anomali in May 2019, and a variant capable of attacking Linux machines was reported in June of this year. This new variant, which Barracuda researchers first detected in late August, is targeting IoT devices, such as TVs that run on Android operating systems, and Linux-based machines, such as routers with ill-configured SSH service.

While the botnet that this malware is building does not have clear functionality yet, it gives the campaign operators a backdoor into the infected devices so they can later be used for cryptomining, DDoS, or other large-scale attacks.

The Details

This variant of InterPlanetary Storm is written in Go, uses the Go implementation of libp2p, and is packed with UPX. It spreads using SSH brute force and open ADB ports, and it serves malware files to other nodes in the network. The malware also enables reverse shell and can run bash shell.

Barracuda researchers found several unique features designed to help the malware persist and protect it once it has infected a machine.

- **It detects honeypots.** The malware looks for the string “svr04” in the default shell prompt (PS1), which was used by the Cowrie honeypot before.
- **It auto updates.** The malware compares the version of the running instance with the latest available version and will update accordingly.
- **It will try to persist itself by installing a service** (system/systemv), using a Go daemon package.

- **It kills other processes on the machine that pose a threat to the malware**, such as debuggers and competing malware. It does so by looking for the following strings in process command lines:
    - “/data/local/tmp”
    - “rig”
    - “xig”
    - “debug”
    - “trinity”
    - “xchecker”
    - “zypinstall”
    - “startio”
    - “startapp”
    - “synctool”
    - “ioservice”
    - “start_”
    - “com.ufo.miner”
    - “com.google.android.nfcguard”
    - “com.example.test”
    - “com.example.test2”
    - “saoas”
    - “skhqwensw”

Interplanetary Storm announced keys

The malware’s backend advertises the following keys into the IPFS Distributed Hash Table (DHT). Infected nodes will then try to find peers that can provide the required services:

Key	Purpose
requeBOHCHIY2XRMYXI0HCSZA	C2
proxybackendH0DHVADBCIKQ4S7YOX4X	Proxy backend
web-api:kYVhV8KQ0mA0rs9pHXoWpD	File distribution backend

Each infected node will advertise the key “fmi4kYtTp9789G3sCRgMZVG7D3uKalwtCuWw1j8LSPHQEGVBU5hfbNdnHvt3kyR1fYUlGNAO0zactmIMIZodsOha9tnfe25Xef1” in order to inform that it is part of the botnet. The ID of each infected machine will be generated once during initial infection and will be reused if the machine restarts or the malware updates.

Infected nodes will also advertise keys in the form “stfadv:<cheksum>” in order to notify that the node can provide a file with that checksum.

Communication protocols

Libp2p applications handle incoming connection (streams) based on a logical address (i.e. unknown to the transport layer) called protocol ID. By convention, protocol ids have a path-like structure, with a version number as the final component.

The following protocol IDs are being used by the malware:

Protocol ID	Purpose	Notes
/sbst/1.0.0	Used for spawning reverse shell	Hosted on nodes
/sfst/1.0.0	Used for file transfer	Hosted on nodes, file checksum is used for the integrity of the served file
/sbpcp/1.0.0	Used for proxy, connect to backend serve	Hosted on backend servers

/sbptp/1.0.0	Used for proxy. Forward proxy channel	Hosted on nodes
/sreque/1.0.0	Used for scanner queue.	Hosted on nodes, commands from the c2 contain signature. Messages on this channel are serialized using JSON objects. Messages from the c2 will be for either “brute-ssh”or “tcp-scan”, directing the node to scan for vulnerable machines. The node will send be the results of these scans. The “brute-ssh” messages from the c2 will include a list of Ips to attack along with the credentials that should be used.

File distribution backend

The file distribution servers can be discovered using the “web-api:kYVhV8KQ0mA0rs9pHXoWpD” key. The relevant peers implement http over the libp2p protocol and serve the following URLs:

Path	Method	Description
/version	GET	Get the peer version
/files/checksum?f=<file name>	GET	Get the current checksum of the file <file name>
/files/seedrs-http?c=<checksum>	GET	Get a list of nodes capable of serving the file
POST /files/seedrs-http	POST	Add node info
/nodes/	POST	Add node info

IOC

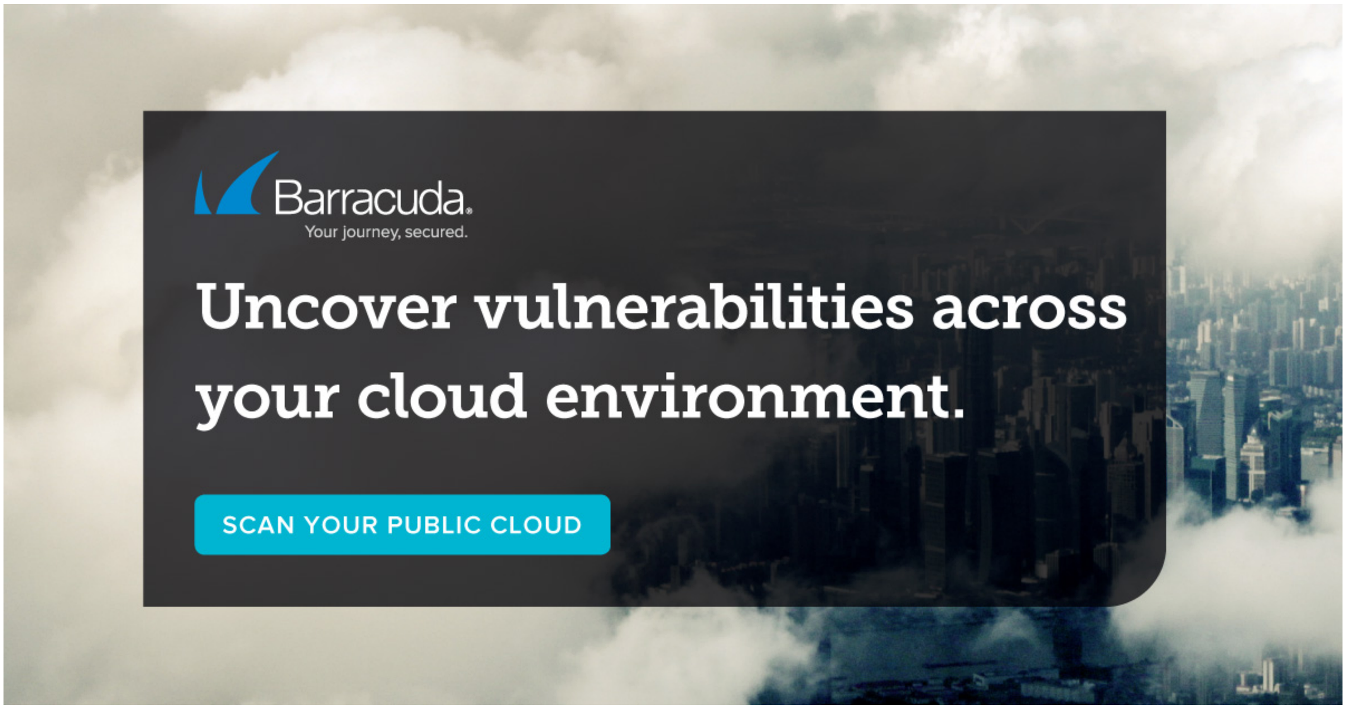
The malware might drop some of the following files:

storm_android-amd64	d4e3102b859ebfda5a276b2ce6f226e27fdcdef5e693ee7742be863236e2374a
storm_android-386	9dab7f5ff2873389a4b0e68cb84978fc5907cd2579bd15a1d39e277f5d2fdc27
storm_android-arm64	16bcb323bfb464f7b1fcfb7530ecb06948305d8de658868d9c3c3c31f63146d4
storm_android-arm7	56c08693fdf92648bf203f5ff11b10b9dcfedb7c0513b55b8e2c0f03b209ec98
storm_linux-amd64	ab462d9d2a9a659489957f80d08ccb8a97bbc3c2744beab9574fda0f74bd1fe2
Storm_linux-386	ba1e8d25cc380fdbbf4b5878a31e5ed692cfd2523f00ca41022e61f76654dd4f
storm_linux-arm64	50406ec7fa22c78e9b14da4ccc127a899db21f7a23b1916ba432900716e0db3d
storm_linux-arm7	a2f4c9f8841d5c02ffd4573c5c91f7711c7f56717ddb981f719256163be986e8
storm_darwin-amd64	4cd7c5ee322e55b1c1ae49f152629bfbdc2f395e9d8c57ce65dbb5d901f61ac1

How to protect against these attacks

There are a few important steps you can take to protect against this malware variant.

- **Properly configure SSH access on all devices.** This means using keys instead of passwords, which will make access more secure. When password login is enabled and the service itself is accessible, the malware can exploit the ill-configured attack surface. This is an issue common with routers and IoT devices, so they make easy targets for this malware.
- **Use a cloud security posture management tool** to monitor SSH access control to eliminate any configuration mistakes, which can be catastrophic. To provide secured access to shells if needed; instead of exposing the resource on the internet, deploy an MFA-enabled VPN connection and segment your networks for the specific needs instead of granting access to broad IP networks.


Barracuda
Your journey, secured.
Uncover vulnerabilities across your cloud environment.
SCAN YOUR PUBLIC CLOUD