



UNC2053



Actor Details

Description:

UNC2053 is a financially motivated cluster of activity that encompasses the use of various loader and backdoor combinations that are distinct but share a common networking protocol. Mandiant has regularly observed these campaigns incorporating new delivery tactics and it is plausible that UNC2053 relies on multiple partners for distribution. We have high confidence that common actors are behind the development of TrickBot and these families. UNC2053 appears to partner with multiple threat actors who leverage access obtained by UNC2053 to subsequently deploy ransomware.

Targeted Industries:

- Aerospace & Defense
- Automotive
- Chemicals & Materials
- Civil Society & Non-Profits
- Construction & Engineering
- Education
- Energy & Utilities
- Financial Services
- Governments
- Healthcare Hospitality
- Insurance
- Legal & Professional Services
- Manufacturing
- Media & Entertainment
- Oil & Gas
- Pharmaceuticals
- Retail
- Technology
- Telecommunications Transportation

Motivations:

Financial Gain

Associated Malware:

-  BEACON
-  BEERBOT
-  BUBBLYBOT
-  CORKBOT
-  EMPIRE
-  GRIMAGENT
-  ICECANDLE
-  KEGTAP
-  METERPRETER
-  POWERTRICK RUMRUNNER
-  SINGLEMALT
-  SPIKEDNOG
-  STILLBOT
-  WINEKEY
- 

Source Regions: 

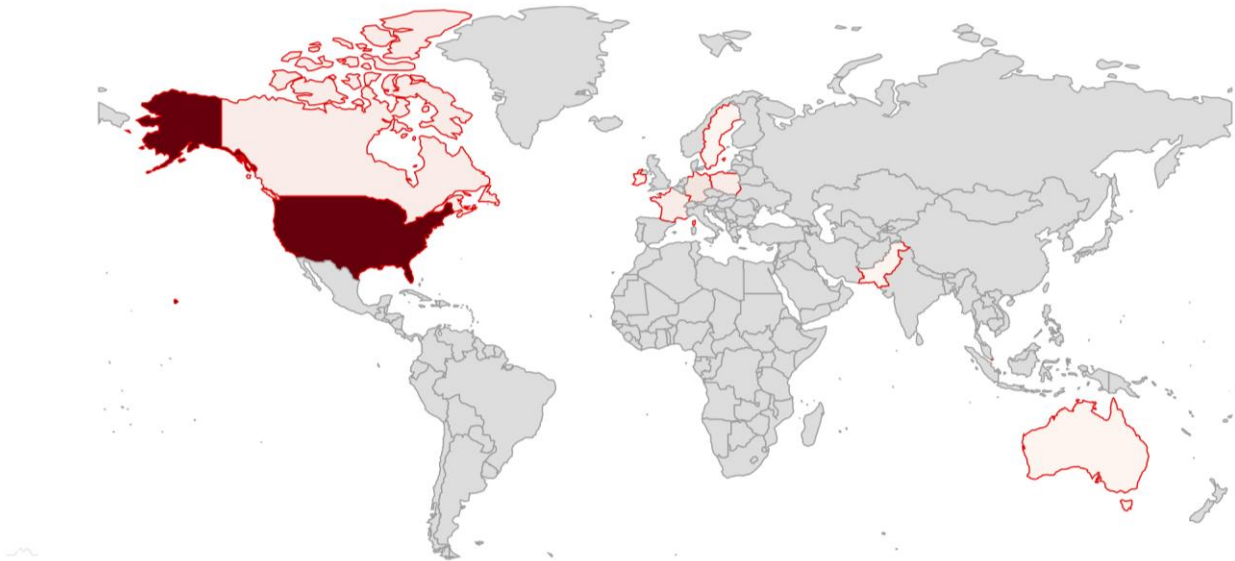
East Europe

Targeted Regions:

- Australia
- Canada
- Colombia
- Denmark
- France
- Germany
- India
- Ireland
- Japan
- Pakistan
- Poland
- Singapore
- Sweden
- United Kingdom
- United States of America

Relevant Reporting:

Targeted Regions | Tracking 10 Regions



Top Results

Displaying 1 of 6 of 10

- United States of America
- Germany
- France
- Canada
- Poland
- Ireland

< 1 2 >



Malware Details

Description:

SPIKEDNOG is a downloader written in C++ that retrieves payloads via HTTP. Payload URLs may be hard-coded or generated using a domain generation algorithm. Downloaded payloads are injected into a separate process and executed. SPIKEDNOG commonly downloads the BUBBLYBOT backdoor.

Operating Systems:

Windows

Role:

Downloader

Capabilities:

Anti-AV: Symantec

Anti-AV: Windows Defender

Anti-AV: eScan

Capture CPU information

Capture disk information

Capture hostname

Communicates using HTTP

Communicates using TLS

Communicates using raw sockets

Constructs mutex

Creates processes

Download files

Encodes using XOR

Lists processes

Lists processes

Performs anti-disassembly obfuscation

Performs process injection

Uses RSA