BAMBOO

▶ CYBER ▶ EYES

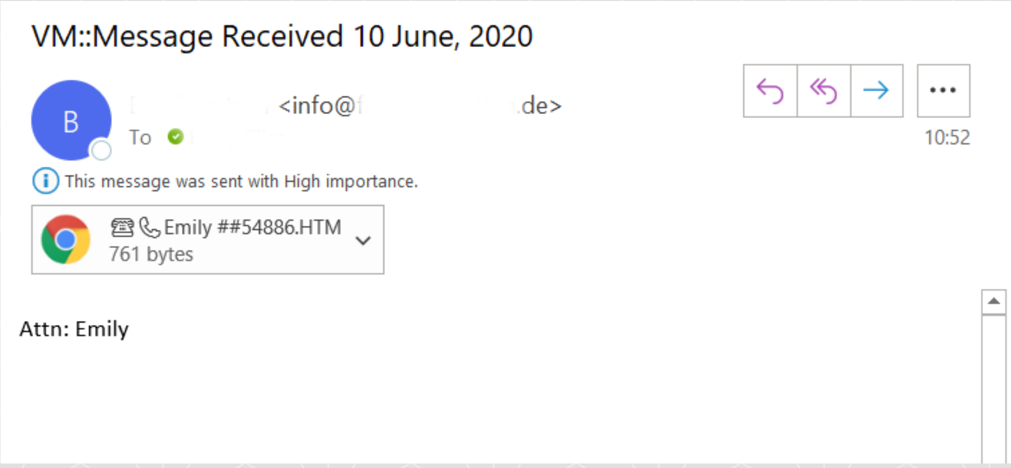
Please see an update of the last few weeks news. Please continue to send useful information on what you are seeing too to cyber@bamboo.tech.

WHAT WE'VE SEEN

Spurious incoming voicemail notifications

There has been a hike in reports of emails of this type. Be sure to check email addresses and other credentials of incoming messages before clicking links.

If unsure, advise your IT department or provider immediately.



VM::Message Received 10 June, 2020

<info@f .de>

To

10:52

This message was sent with High importance.

☎📞Emily ##54886.HTM
761 bytes

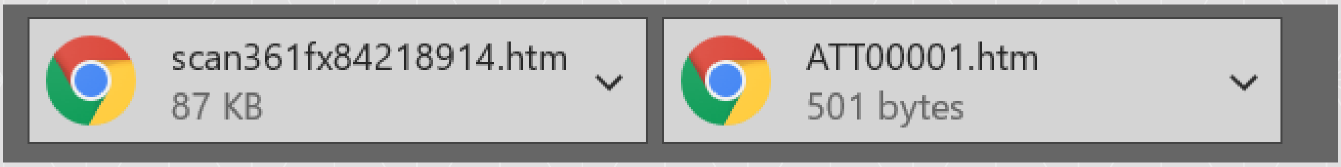
Attn: Emily

WHAT WE'VE HEARD ABOUT

Incoming emails referencing scanned documents for your attention.

From – Docu.....<email address here needs to be looked at closely>
Date: 15 June 2020 at 21:36:54 BST
To: Your name and standard email address
Subject ref: New Scanned file–4H4XPTHHJ8 From your contact

Files to open look as follows:



scan361fx84218914.htm
87 KB

ATT00001.htm
501 bytes

For further information or indicators of compromise please email cyber@bamboo.tech

WHAT WE'VE BEEN MADE AWARE OF

Ransomware

Snake is a new ransomware family that targets enterprise networks. The malware is written in Go and contains a much higher level of obfuscation than is typically associated with the targeted approach. Upon successful infection, Snake deletes the system's Shadow Volume Copies and kills numerous processes related to SCADA systems, virtual machines, industrial control systems, remote management tools, network management software and more.

The ransomware then encrypts all files on the device with the exception of those located in the Windows system folders and various other system files. Encrypted files receive a random fivecharacter string extension. The ransomware also appends the EKANS (SNAKE in reverse) file marker to each file. Snake then creates a ransom note on the desktop that contains instructions to contact a provided email address, bapcocrypt@ctemplar.com, for payment instructions.

This threat affects Windows operating systems.

Ransomware-as-a-service

Thanos is a new ransomware-as-a-service (RaaS) available on underground forums from a user under the alias "Nosophoros". Thanos is written in C# and provides 43 different configuration options. While straightforward, the ransomware does incorporate some advanced features such as the RIPlace technique. Thanos continues to rise in popularity largely due to its ready-to-use nature.

The RIPlace technique emerged as a proof of concept from a security company in late 2019. The technique bypasses most existing anti-ransomware methods and can evade antivirus products. This implementation is noteworthy as it demonstrates an in-the-wild instance of a threat actor weaponizing a proof of concept originating from security research.

Thanos' general execution path contains three main activities:

1. Advanced Options: performs actions related to the configuration settings

2. Prevent Termination and Recovery: stops services and processes that prevent its ability
to run and delete backup files and shadow copies

3. Encrypt and Upload: encrypt files and upload to FTP if configured to do so at build time
and show the ransom note

This threat affects Windows operating systems.

TALK ABOUT TECH

What is a brute force attack?

A brute force attack, aka, an exhaustive search, is a hack that works by calculating every possible combination of a target password until the correct password is discovered.

As the password's length increases, the amount of time, on average, to find the correct password increases exponentially.

Other types of attack may use a list of commonly used passwords. If your password is 'password', for example, a brute force bot would be able to crack your password within seconds.

Stay Connected

Stay Vigilant

Stay Secure

For further information or indicators of compromise please email cyber@bamboo.tech