Deceptive Bytes

Active Endpoint Cyber Defense

Prevention by Deception

Case Study
Emotet Attack on
Events Services Provider

Customer Profile

Our customer is an important company in the events services sector located in West Europe, which has always been attentive to investments in technology and IT security issues. The protection of internal systems, data, customer registration and transactions that purchase access tickets with online ticketing systems are the priorities that have led the company to make choices of maximum security and to anticipate possible options with innovative solutions against cyber-attacks.

Need

At the end of 2019 - early 2020, after the news of attacks on other events services organizations, the spread of the pandemic and the need to operate in smart working, and given the increase in the potential attack surface and vulnerability, the company has chosen with farsightedness to implement - on top of security solutions at the highest levels already implemented - innovative cyber-security solutions able to protect and, above all, to further prevent the company and employees themselves from potential attacks in continuous evolution.

Overview

In fact, every day, all over the world, malware attacks organizations and companies of all sizes, affecting their daily activities and causing losses to companies that can be significant. Malware is highly intelligent and evasive and uses several techniques to evade detection and analysis by security systems and researchers. Furthermore, the APT groups that launch mass email spam campaigns by randomly infecting users and with the help of careless or hasty employees, are now supported by evolved attack operators who work in vertically organized structures. Malware botnet operators often rely on social engineering to trick users into installing malware on their systems, even if the computers are running up-to-date Antivirus software.

How Emotet Malware Works

Like in many organizations that experienced an Emotet attack, this type of malware comes into the network via a phishing email that contains an encrypted, password-protected file. The user unlocks the file, which “detonates” the malware, this enables it access to the endpoint & network, ultimately spreading malware through the network. As it spreads across the network, it contacts its Command & Control servers (C2) to dynamically mutate the executable file to evade traditional malware detection and remediation tools. Emotet is later used by cyber criminals to perform DDoS attacks as part of a Botnet network, Ransomware attacks as a secondary payload, or as a banking trojan to steal banking/ financial information.

© Copyright of Deceptive Byte Ltd., 2021 - All Rights Reserved

Solution

Shaping the attackers' decision making

Deceptive Bytes provides a fully endpoint-centric deception platform that uses existing IT infrastructure, responds to the evolving nature of advanced threat landscape and interferes with attackers attempts to recon & take hold of enterprise IT, in a preventative solution which covers sophisticated malware techniques & defenses in several ways...

Preemptive Defense:
Making malware believe it's in an unattractive/hostile environment to attack, reducing its motivation to attack and the chance of infection.

Proactive Defense:
Dynamically responding to threats as they evolve, based on the current detected stage of compromise, and changing the outcome of the attack.

> *"Prevention is better than cure, said an old advertisement.... With the Deceptive Bytes solution and the support of our IT security service provider, we have added a level of protection, but above all of prevention of attacks, guaranteeing our systems a very high level of security."*

Director of Information Systems, Events Services Provider

Incident

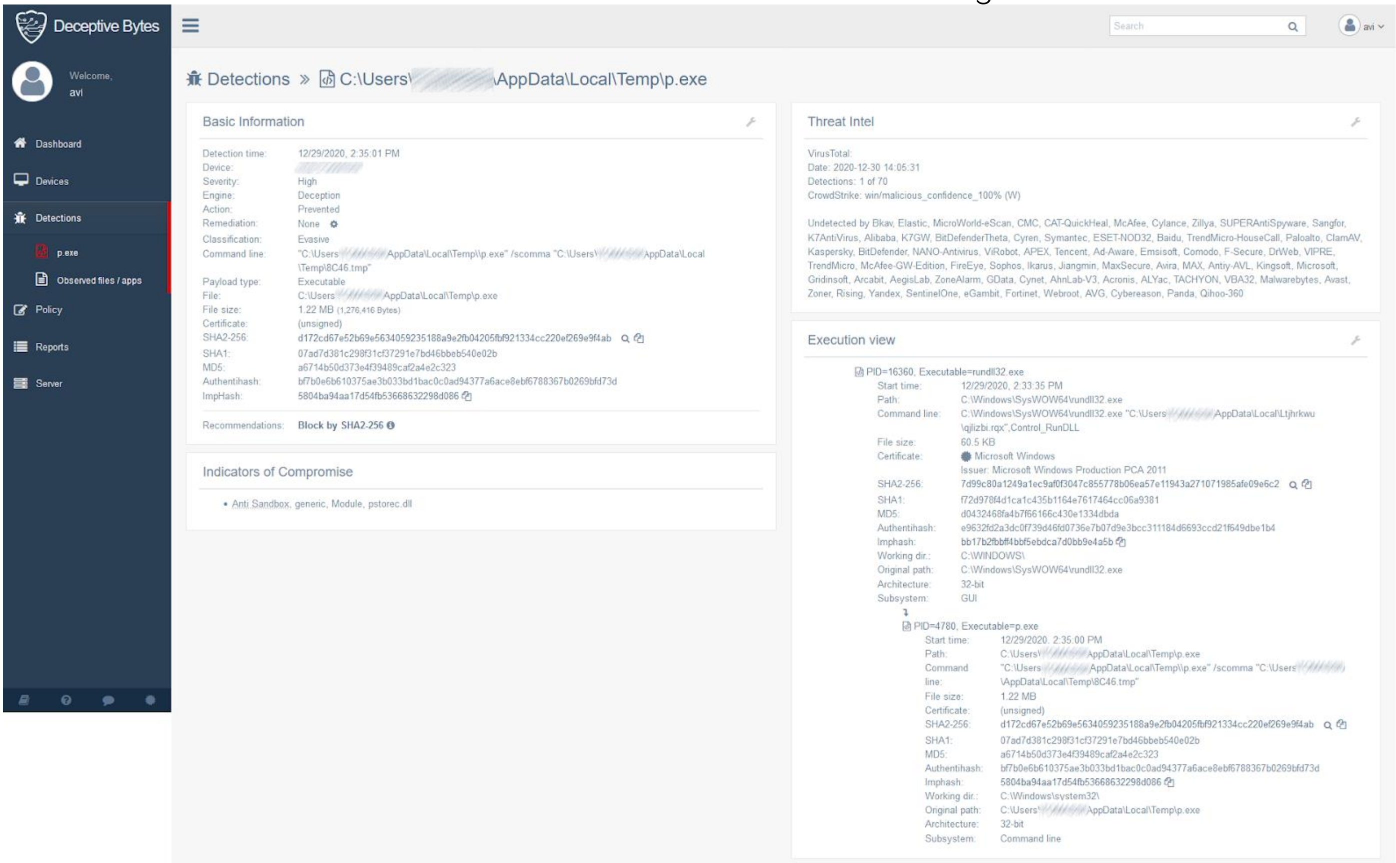
During the holiday season, which is a time when attacks are increasing due to lack of attention & monitoring, a user opened a malicious email that contained Emotet, thinking it was a legitimate password protected tender document (directed to the company). He enabled the macro in the Word file which initiated the malware attack. Due to the customer's configuration, detecting 1st stage payloads (protecting Office in this case) was off, so the document executed a malicious PowerShell code that downloaded & started an executable file. The agent then detected the execution of the unknown file and activated the Deception engine on it, which detected the malicious executable (2nd stage payload) & neutralized the threat immediately.

Conclusion

Deceptive Bytes' solution provided immediate prevention capabilities to the customer while the user mistakenly opened a malicious file. The solution operated automatically without operator intervention, reducing the prevention & detection dwell time to zero, and safeguarding the organization from an unknown attack and potentially, any mutation of it.
Deceptive Bytes' team alerted the customer & service provider about the incident, which allowed them the ability to further investigate the malware at their convenience and remove any other related threat while keeping the organization secure.

© Copyright of Deceptive Byte Ltd., 2021 - All Rights Reserved

Prevention & detection information as shown from the customer's management server



Detections » C:\Users\[redacted]\AppData\Local\Temp\p.exe

Basic Information

Detection time: 12/29/2020, 2:35:01 PM
Device: [redacted]
Severity: High
Engine: Deception
Action: Prevented
Remediation: None
Classification: Evasive
Command line: "C:\Users[redacted]AppData\Local\Temp\\p.exe" /scomma "C:\Users\[redacted]AppData\Local\Temp\8C46.tmp"
Payload type: Executable
File: C:\Users[redacted]AppData\Local\Temp\p.exe
File size: 1.22 MB (1,276,416 Bytes)
Certificate: (unsigned)
SHA2-256: d172cd67e52b69e5634059235188a9e2fb04205fbf921334cc220ef269e9f4ab
SHA1: 07ad7d381c298f31cf37291e7bd46bbeb540e02b
MD5: a6714b50d373e4f39489caf2a4e2c323
Authentihash: bf7b0e6b610375ae3b033bd1bac0c0ad94377a6ace8ebf6788367b0269bfd73d
ImpHash: 5804ba94aa17d54fb53668632298d086

Recommendations: **Block by SHA2-256**

Indicators of Compromise

- Anti Sandbox, generic, Module, pstorec.dll

Threat Intel

VirusTotal:
Date: 2020-12-30 14:05:31
Detections: 1 of 70
CrowdStrike: win/malicious_confidence_100% (W)

Undetected by Bkav, Elastic, MicroWorld-eScan, CMC, CAT-QuickHeal, McAfee, Cylance, Zillya, SUPERAntiSpyware, Sangfor, K7AntiVirus, Alibaba, K7GW, BitDefenderTheta, Cyren, Symantec, ESET-NOD32, Baidu, TrendMicro-HouseCall, Paloalto, ClamAV, Kaspersky, BitDefender, NANO-Antivirus, ViRobot, APEX, Tencent, Ad-Aware, Emsisoft, Comodo, F-Secure, DrWeb, VIPRE, TrendMicro, McAfee-GW-Edition, FireEye, Sophos, Ikarus, Jiangmin, MaxSecure, Avira, MAX, Antiy-AVL, Kingsoft, Microsoft, Gridinsoft, Arcabit, AegisLab, ZoneAlarm, GData, Cynet, AhnLab-V3, Acronis, ALYac, TACHYON, VBA32, Malwarebytes, Avast, Zoner, Rising, Yandex, SentinelOne, eGambit, Fortinet, Webroot, AVG, Cybereason, Panda, Qihoo-360

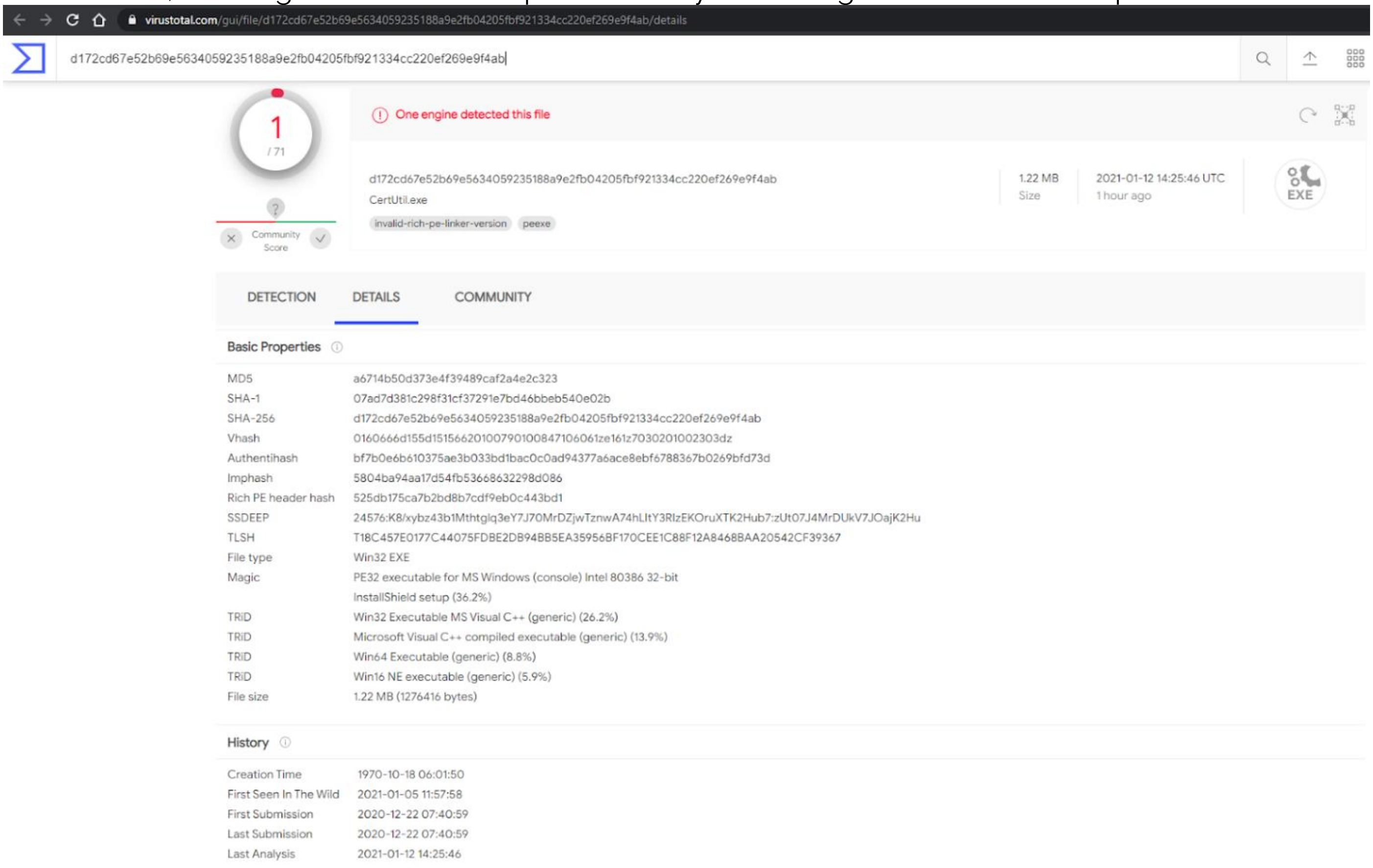
Execution view

PID=16360, Executable=rundll32.exe
Start time: 12/29/2020, 2:33:35 PM
Path: C:\Windows\SysWOW64\rundll32.exe
Command line: C:\Windows\SysWOW64\rundll32.exe "C:\Users[redacted]AppData\Local\Ltjhrkwu\qjlizbi.rqx",Control_RunDLL
File size: 60.5 KB
Certificate: Microsoft Windows
Issuer: Microsoft Windows Production PCA 2011
SHA2-256: 7d99c80a1249a1ec9af0f3047c855778b06ea57e11943a271071985afe09e6c2
SHA1: f72d978f4d1ca1c435b1164e7617464cc06a9381
MD5: d0432468fa4b7f66166c430e1334dbda
Authentihash: e9632fd2a3dc0f739d46fd0736e7b07d9e3bcc311184d6693ccd21f649dbe1b4
Imphash: bb17b2fbbff4bbf5ebdca7d0bb9e4a5b
Working dir.: C:\WINDOWS\
Original path: C:\Windows\SysWOW64\rundll32.exe
Architecture: 32-bit
Subsystem: GUI

PID=4780, Executable=p.exe
Start time: 12/29/2020, 2:35:00 PM
Path: C:\Users\[redacted]AppData\Local\Temp\p.exe
Command line: "C:\Users[redacted]AppData\Local\Temp\\p.exe" /scomma "C:\Users[redacted]\AppData\Local\Temp\8C46.tmp"
File size: 1.22 MB
Certificate: (unsigned)
SHA2-256: d172cd67e52b69e5634059235188a9e2fb04205fbf921334cc220ef269e9f4ab
SHA1: 07ad7d381c298f31cf37291e7bd46bbeb540e02b
MD5: a6714b50d373e4f39489caf2a4e2c323
Authentihash: bf7b0e6b610375ae3b033bd1bac0c0ad94377a6ace8ebf6788367b0269bfd73d
Imphash: 5804ba94aa17d54fb53668632298d086
Working dir.: C:\Windows\system32\
Original path: C:\Users\[redacted]AppData\Local\Temp\p.exe
Architecture: 32-bit
Subsystem: Command line

Threat Intel

The file, as it appeared on VirusTotal, seems to be undetected by all other vendors except CrowdStrike, allowing threat actors to spread it easily across organizations uninterrupted.



virustotal.com/gui/file/d172cd67e52b69e5634059235188a9e2fb04205fbf921334cc220ef269e9f4ab/details

d172cd67e52b69e5634059235188a9e2fb04205fbf921334cc220ef269e9f4ab

One engine detected this file

d172cd67e52b69e5634059235188a9e2fb04205fbf921334cc220ef269e9f4ab
CertUtil.exe
invalid-rich-pe-linker-version peexe

1.22 MB
Size

2021-01-12 14:25:46 UTC
1 hour ago

Basic Properties

MD5	a6714b50d373e4f39489caf2a4e2c323
SHA-1	07ad7d381c298f31cf37291e7bd46bbeb540e02b
SHA-256	d172cd67e52b69e5634059235188a9e2fb04205fbf921334cc220ef269e9f4ab
Vhash	0160666d155d15156620100790100847106061ze161z7030201002303dz
Authentihash	bf7b0e6b610375ae3b033bd1bac0c0ad94377a6ace8ebf6788367b0269bfd73d
Imphash	5804ba94aa17d54fb53668632298d086
Rich PE header hash	525db175ca7b2bd8b7cdf9eb0c443bd1
SSDEEP	24576:K8/xybz43b1Mthtglq3eY7J70MrDZjwTznwA74hLItY3RlzEKOruXTK2Hub7:zUt07J4MrDUkV7JOajK2Hu
TLSH	T18C457E0177C44075FDBE2DB94BB5EA35956BF170CEE1C88F12A8468BAA20542CF39367
File type	Win32 EXE
Magic	PE32 executable for MS Windows (console) Intel 80386 32-bit
	InstallShield setup (36.2%)
TRiD	Win32 Executable MS Visual C++ (generic) (26.2%)
TRiD	Microsoft Visual C++ compiled executable (generic) (13.9%)
TRiD	Win64 Executable (generic) (8.8%)
TRiD	Win16 NE executable (generic) (5.9%)
File size	1.22 MB (1276416 bytes)

History

Creation Time	1970-10-18 06:01:50
First Seen In The Wild	2021-01-05 11:57:58
First Submission	2020-12-22 07:40:59
Last Submission	2020-12-22 07:40:59
Last Analysis	2021-01-12 14:25:46

© Copyright of Deceptive Byte Ltd., 2021 - All Rights Reserved

About Deceptive Bytes

Deceptive Bytes, a leader in endpoint deception technology, provides its Active Endpoint Deception platform to enterprises & MSSPs which enables them real-time prevention of unknown and sophisticated threats. The solution dynamically responds to threats as they evolve, based on the current detected stage of compromise and changes their outcome, giving defenders the upper-hand in protecting their assets and data.

Recognized as a Gartner Cool Vendor in Security Operations and Threat Intelligence, 2019 report.

Additional information

Website LinkedIn Twitter Facebook info@deceptivebytes.com

© Copyright of Deceptive Byte Ltd., 2021 - All Rights Reserved