Check Point's Threat Emulation Stops Large-Scale Phishing Campaign in Germany

By bferrite

Published: 2019-06-19 · Archived: 2026-04-10 02:46:20 UTC

Research by: Kobi Eisenkraft, Moshe Hayun, published June 19th 2019

Introduction

During the first week of June 2019, Check Point researchers encountered a new, large-scale phishing campaign targeting German companies across all industries. The hacker's goal was to install Remcos – a remote control tool – on the victims' computers.

Attack Flow

The attackers initially sent fake emails that appeared to be from several legitimate companies across Germany. These emails contained invoices or urgent order attachments which were actually Remcos archives attempting to connect with the attacker's command and control (C&C) server.

Figure 1: Example of a phishing email to the victims

The attachment is usually an archive containing an executable disguised as a PDF or other document file. The disguise is a simple comma PDF extension and folder icon.

Figure 2: An executable in disguise

After the victim opens the file, Remcos executes silently and gives the attacker full control over the victim's machine.

Figure 3: Attack flow chart

Communication with the C&C

The attacker then covers his tracks by using DDNS (Dynamic DNS), a legitimate service for mapping Internet domain names to dynamic IP addresses. Learn more about this well-known evasion technique at: https://attack.mitre.org/techniques/T1311/.

By using free DDNS accounts, the attacker has a large number of IP addresses at their disposal and can use them to control the victims' machines.

For example, the attacker uses https://www.noip.com/ service to create the domain ablegod.hopto[.]org.

Remcos – a Swiss Army Knife RAT

Figure 4: Picture from the official Remcos website

Distributed and sold as a legitimate tool by a company called “Breaking Security” on a public website, Remcos is an abbreviation for Remote Control and Surveillance and is sold on a fremium model with a pro version priced from €58 – €389.

By using Remcos, the attacker can remotely gain full control of another machine and include the following functions:

Bypass AV products and privilege escalation:

- Gain admin privileges
- Disable UAC (User Account Control)
- Maintain persistence on the targeted machine
- Run as a legitimate process (e.g. injection to Windows process)
- Run in the background, invisible to the victim

Capabilities:

- Keylogger and clipboard
- ScreenLogger
- Audio capture
- Extract passwords

Figure 5: Campaign targeting Germany and other countries. 5/6 – 6/6

Check Point products successfully protect against this campaign.

Check Point Threat Emulation is a Zero-Day Protection solution that prevents infections from zero-day malware and targeted attacks using sandboxing capabilities.

Check Point SandBlast Agent provides purpose-built advanced Zero-Day Protection capabilities to protect web browsers and endpoints, leveraging Check Point’s industry leading network protections.

Protections:

Check Point Threat Emulation:

- RAT.Win.Remcos.A
- RAT.Win.Remcos.C
- RAT.Win.Remcos.D

Check Point SandBlast Agent:

- RAT.Win.Remcos.B

Figure 6: Threat emulation report blocking Remcos

The full Threat Emulation report can be found here –

https://forensics.checkpoint.com/remcos_te/ThreatEmulationReport.html

The full SBA report can be found here –

https://forensics.checkpoint.com/remcos/index.html

A special thanks to our colleague Arie Olshtein for his contribution on this research!

Indicators of Compromise:

- 303b30ca9d902de72ce83e2b53a496ab2275e4ab58f1151bed1484f421ecc0fa
- 97732c98efbaba02b124439795b3b90985ee0aba906021d5c0a348c79f866230
- c0808c63274677a56177fda9f78ce04bb35e0190740acb2ed268b23a0943ef35
- a4f06a387a1c920d6ebec1098f410879fdf8d9f983209f7e8102a1c6d4b459e9
- 5a9922e81bce762658f36f7d1946a02d63c0430d0b29caf3ee5f70ab7dfd40f2
- 7a5aaecbf18cc78f77f307391716af241313f37eeb5a5fb4080c66574aa6b470
- 568172c320330ceb592add095493beee53446a0310dbf894d2f8f6a1cc4080f3
- dc607b53277b8a0b83dee0b2893d50df0edb5550f94b88381b614ddc163ebe66
- e3cc136991d5c302aeef3f75712ac93f4c4eaf88425494511aaafcfc5247fad5
- 874d254f69efa9193d96c0dbec74b5995f84f9253ba8524e0cfe0f7f612bfb62
- 3f8fa4dc5fcbef7c853a85e9abefbe78b2da3275b96a4288db871453a0a4b853
- 48813f9c61687fb59ca606160b24b1b560d43152ee8fb09692475dd8ac5871f1
- a02b84b2c2fad7ba6ccd785017e5f64fe9bd1251fc3fb3cc04175d5a904568b1
- amblessed.ddns[.]net
- ableyahweh.ddns[.]net
- uaeoffice999.warzonedns[.]com
- pmv1515.duckdns[.]org
- forbbma.ddns[.]net
- alexthomas.ddns[.]net
- timmy66.ddns[.]net
- timmy55.ddns[.]net
- ablegod.hopto[.]org
