|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Template "Angriffsanalyse"

1. Januar 2020

 Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | TMP400006 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung (vergeben] |
| Name des Dokuments |  | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 5 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc87774351)

[Dokumentenhistorie 3](#_Toc87774352)

[Inhaltsverzeichnis 4](#_Toc87774353)

[Arbeitsblatt zur Angriffsanalyse/suche 5](#_Toc87774354)

[Analyse der Kill Chain 5](#_Toc87774355)

[Delivery 5](#_Toc87774356)

[Exploitation 5](#_Toc87774357)

[Installation 6](#_Toc87774358)

[Command und Control 6](#_Toc87774359)

[Zusammenfassung 6](#_Toc87774360)

Arbeitsblatt zur Angriffsanalyse/suche

|  |  |
| --- | --- |
| Name: |  |
| Datum: |  |

Analyse der Kill Chain

**Aufklärung (betroffenes System)**

**Patient Zero: System- und Benutzerinformationen**

|  |  |
| --- | --- |
| Computername: |  |
| Betriebssystem: |  |
| Gefährdete Anwendungen: |  |
| Eingeloggter Benutzername: |  |
| MAC Adresse: |  |
| Host IP-Adresse(n): |  |

Delivery

**Angreifer-Infrastruktur und Dropper-Datei**

|  |  |
| --- | --- |
| Malicious Domains: |  |
| Dropper Dateinamen: |  |
| IP-Adresse(n): |  |
| Dropper Dateityp: |  |

Exploitation

**Infektionsvektor**

|  |  |  |  |
| --- | --- | --- | --- |
| E-Mail | Anhang | Ja/nein | <wenn zutreffend kurze Beschreibung> |
| Phishing Link | Ja/nein | <wenn zutreffend kurze Beschreibung> |
| Web | Exploits Kit | Ja/nein | <wenn zutreffend kurze Beschreibung> |
| Phishing Link | Ja/nein | <wenn zutreffend kurze Beschreibung> |
| Active Exploitation | Ja/nein | <wenn zutreffend kurze Beschreibung> |
| Andere Methode | Ja/nein | <wenn zutreffend kurze Beschreibung> |

Installation

**Malware Binary**

|  |  |
| --- | --- |
| Dateinamen: |  |
| Name der Malware Familie: |  |
| Dateityp: |  |

Command und Control

**Command and Control (C2) Communications**

|  |  |
| --- | --- |
| Kontaktierte Domains: |  |
| Kontaktierte URLs: |  |
| Kontaktierte IPs: |  |

**Maßnahmen zur Zielerreichung**

**Spuren des Angriffs**

|  |  |
| --- | --- |
| Prozessinjektion entdeckt: | <wenn ja, welcher Prozess> |
| Eskalation von Privilegien festgestellt: | <wenn ja, welche Methode> |
| PowerShell / Scripting-Befehle erkannt: | <wenn ja, bitte auflisten> |
| Bekannte Malware Funktionen erkannt: | <wenn ja, bitte auflisten> |

Zusammenfassung

|  |  |
| --- | --- |
| Datum/Uhrzeit der Erstinfektion des Patienten Zero: |  |
| Gesamtzahl der betroffenen Systeme: |  |
| Zeitstrahl: |  |
| Sicherheitsempfehlungen: |  |