# HE Semesterarbeit Malware Analyse

Sie recherchieren und analysieren in einer Gruppenarbeit zu einer der drei Ransomware Familien *Emotet*, *Petya* oder *WannaCry*.

Ziel ist es, dass Sie anhand eines konkreten Beispieles den Ablauf eines Malwarebefalls kennen und rekonstruieren können. Sie setzen sich mit der Materie eines Angriffes auseinander und analysieren mögliche Massnahmen, die einen solchen Angriff verhindert hätten.

## Terminplan

- März: Ausgabe der Semesterarbeit
- Sie sprechen sich ab und verteilen sich auf die drei Gruppen wobei es keine Einzelarbeiten gibt und nennen spätestens am zweiten Abend (HE2) dem Dozenten Ihr Thema und Ihre Gruppenmitglieder.
- 26. Mai: Abgabe Ihrer Arbeit bis spätestens 23:59 Uhr

## Vorgaben

### Dokument

- PDF-Datei: <Ransomeware Familie>_<nachname_1>_<nachname_n>.pdf
- Abgabe aller Dokumente in einem passwortgeschützten ZIP (Passwort: hackingExposed) per Mail an ahmet.inci @ juventus.schule und zusätzlich in der File-Ablage von OpenOlat.
  - Mails mit Malware-Namen scheinen teilweise gefiltert zu werden, deshalb das Passwort-ZIP und die zusätzliche Verwendung der File-Ablage.

### Inhalt

- Allgemeine Beschreibung der Malware
  - Wie heisst die Malware und was macht sie? Wann wurde sie zuerst / zuletzt gesichtet? Wie ordnen Sie diese Malware im Vergleich zu anderer Malware ein? Woher stammt die Malware (vermutlich)? Gegen wen wurde die Malware eingesetzt und mit welchem Zweck?
- Beschreibung eines konkreten Malwarebefalls
  - Beschreiben Sie den Angriffsvektor und den Ablauf eines erfolgreichen Angriffes wenn möglich am Beispiel eines konkreten, öffentlich bekannten Vorfalles.
  - Geben Sie an, wie das Opfer wieder vom Angriff befreit werden konnte.
- Illustration
  - Erstellen Sie ein Kontext-Diagramm welches Ihre Beschreibung der aktivitäten der Malware graphisch verdeutlicht. Sie sind frei in der Form und Gestalltung.
- Abwehrmassnahmen
  - Überlegen Sie sich, wie man sich vor diesem Angriff schützen kann und begründen Sie Ihre Massnahmen.
  - Keine Allgemeinplätze die immer gültig sind wie bspw. «Backup der Daten machen», «Virenscanner in aktueller Version einsetzen» oder «sichere Passwörter verwenden».

## Bewertung

Diese Arbeit wird benotet. Die Benotung erfolgt nach folgendem Raster und zählt zusammen mit der Theorie-Prüfung und den Laboraufgaben zur Modulnote. Plagiate und nicht termingerechte Einreichungen werden mit der Note 1 bewertet.

| **Kriterium** | **Punkte** |
|---|---|
| Allgemeine Beschreibung der Malware<br>*Ist die allgemeine Beschreibung der Malware übersichtlich, vollständig und kompakt vorhanden?* | 3 |
| Beschreibung eines konkreten Malwarebefalls<br>*Wurde der Angriff, die daraus resultierenden Konsequenzen und die Behebung des Angriffes korrekt beschrieben?* | 3 |
| Illustration<br>*Hilft die Illustration die Aktivitäten der Malware besser zu verstehen? Ist sie klar strukturiert und sind wichtige Aspekte verständlich (Abfolge der Aktionen, Beschriftung der Komponenten etc.)?* | 3 |
| Abwehrmassnahme<br>*Ist die Beschreibung der Abwehrmassnamen vollständig, korrekt und logisch begründet? Wurden sinnvolle Abwehrmassnahmen vorgeschlagen? Sind die Abwehrmassnahmen verständlich begründet?* | 3 |
| Quellen sauber deklariert<br>*Sind korrekte und sinnvolle Quellen angegeben?* | 3 |
| Vorgaben eingehalten<br>*Wurden alle Vorgaben korrekt eingehalten? Ist der Umfang der Einreichung den Vorgaben entsprechend?* | 3 |
| Rechtschreibung & Stil<br>*Ist die Zusammenfassung fehlerfrei und verständlich formuliert?* | 3 |

Skala: 3 Punkte sehr gut, 2 Punkte gut, 1 Punkt genügend, 0 Punkte ungenügend