Malware "Urausy narrt User mit gefakten Zahlungsaufforderungen

Malware "Urausy" narrt User mit gefakten Zahlungsaufforderungen

AlienVault Labs-Team analysiert Ransomware-Familie
Kürzlich hat Security-Experte AlienVault die Urausy-Familie in seinem Labs genauer unter die Lupe genommen. Die Schädlinge zählen zur Ransomware: Schadprogramme, die Zugriffe auf oder die Nutzung von Daten sowie des gesamten Computers verhindern. Sie verbreiten sich über Exploit-Kits wie Blackhole, die Schwachstellen in Webbrowsern, Flash oder Java ausnutzen. Über diese Lecks installieren sie bösartige Software auf kompromittierten Rechnern. Infizierte Computer sperren plötzlich den Bildschirm und verlangen eine Geldstrafe einer angeblich rechtmäßigen Strafverfolgungsbehörde an. Erst nach Zahlung solle der Rechner wieder ordnungsgemäß arbeiten.
Hinter diesem Angreifer steckt eine Scam-Attacke. Die AlienVault-Experten weisen darauf hin, dass Strafverfolgungsbehörden zum einen niemals den Computer auf diese Weise sperren würden und zum anderen keinesfalls Geld verlangen. Ist der Rechner erst einmal infiziert, führt sich die Malware automatisch aus. Dabei ist sie so geschrieben, dass sie vor der Entdeckung durch Antiviren-Software geschützt ist. Außerdem verfügt der Schädling über mehrere Anti-Analyse-Tricks, um Debugging (Fehlersuche) und Ausführung in Sandbox-Umgebungen zu verhindern. Dazu prüft der Urausy-Threat, ob er unter den wachsamen Augen eines Debuggers läuft und kann ggf. seine Verhaltensweise verändern.
Kontrolle über die gesamte UI
Sobald sie gestartet wurde, injiziert sich die Malware in den Windows-Prozess svchost, kopiert sich in "C:Documents and SettingsAdministratorApplication Dataskype.dat und richtet eine .ini- Datei in "C:Documents and SettingsAdministratorApplication Dataskype.ini ein. Dadurch wird das Schadprogramm direkt beim Systemstart geladen. Danach verhält die Malware sich zunächst ruhig, um der Erkennung zu entgehen. Schließlich zeigt der Schädling den gesperrten Bildschirm an, was er mittels "CreateDesktopW" und "CreateWindowEx" schafft. Sie verschaffen ihm Kontrolle über die komplette Benutzeroberfläche.
Betroffenen Usern stellt AlienVault eine YARA-Regel zum Download bereit, um gegen infizierte Speicherprozesse vorzugehen. Sie steht unter https://github. com/jaimeblasco/AlienvaultLabs/blob/master/malware_analysis/Urausy/urausy_skypedat.yar zum kostenfreien Download bereit. Darüber hinaus schützt die von AlienVault entwickelte Unified Security Management-Plattform AV-USM vor diesen und weiteren Schädlingen aus dem Bereich Ransomware.
Weitere Informationen zu Urausy stehen im Blog der AlienVault Labs bereit.
Über AlienVault:
Die Unified Security ManagementTM-Plattform AV-USM von AlienVault ebnet Unternehmen mit eingeschränktem Security-Personal und Budget einen schnellen und kostengünstigen Weg, Anforderungen an Compliance und Threat Management zu erfüllen. Da alle essenziellen Kontrollfunktionen bereits integriert sind, verschafft die AV-USM gerade kleinen Security-Teams eine Enterprise-Class-mäßige Security-Umgebung. AlienVaults Open Threat ExchangeTM, ein System für den Austausch zum Thema Threat Intelligence zwischen OSSIM-Nutzern und AlienVault-Kunden, stellt dabei sicher, dass AV-USM den Bedrohungen stets einen Schritt voraus ist. AlienVault ist ein Privatunternehmen mit Hauptsitz in Silicon Valley (Kalifornien/USA) und wird von Kleiner Perkins Caufield
 Byers, Sigma, Trident Capital und Adara Venture Partners unterstützt. Die Märkte in Deutschland, Österreich und der Schweiz werden von der AlienVault Deutschland GmbH mit Sitz in Ismaning betreut. Für weitere Informationen besuchen Sie www.alienvault.com oder folgen Sie uns auf Twitter.

AlienVault Deutschland GmbH
Gutenbergstraße 6
D-85737 Ismaning
 www.alienvault.com
Oliver Bareiss
Regional Director DACH and Central Europe
Tel.: +49 (0) 89-32 60 70 91
Fax: +49 (0) 89-97 89 93 42
E-Mail: obareiss@alienvault.com
Sprengel
 Partner GmbH
Nisterstraße 3
D-56472 Nisterau
 www.sprengel-pr.com
Fabian Sprengel
Tel.: +49 (0) 26 61-91 26 0-0
Fax: +49 (0)26 61-91 26 0-29
E-Mail: alienvault@sprengel-pr.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=536439" width="1" height="1">

Pressekontakt

AlienVault Deutschland GmbH

85737 Ismaning

obareiss@alienvault.com

Firmenkontakt

AlienVault Deutschland GmbH

85737 Ismaning

obareiss@alienvault.com

Weitere Informationen finden sich auf unserer Homepage