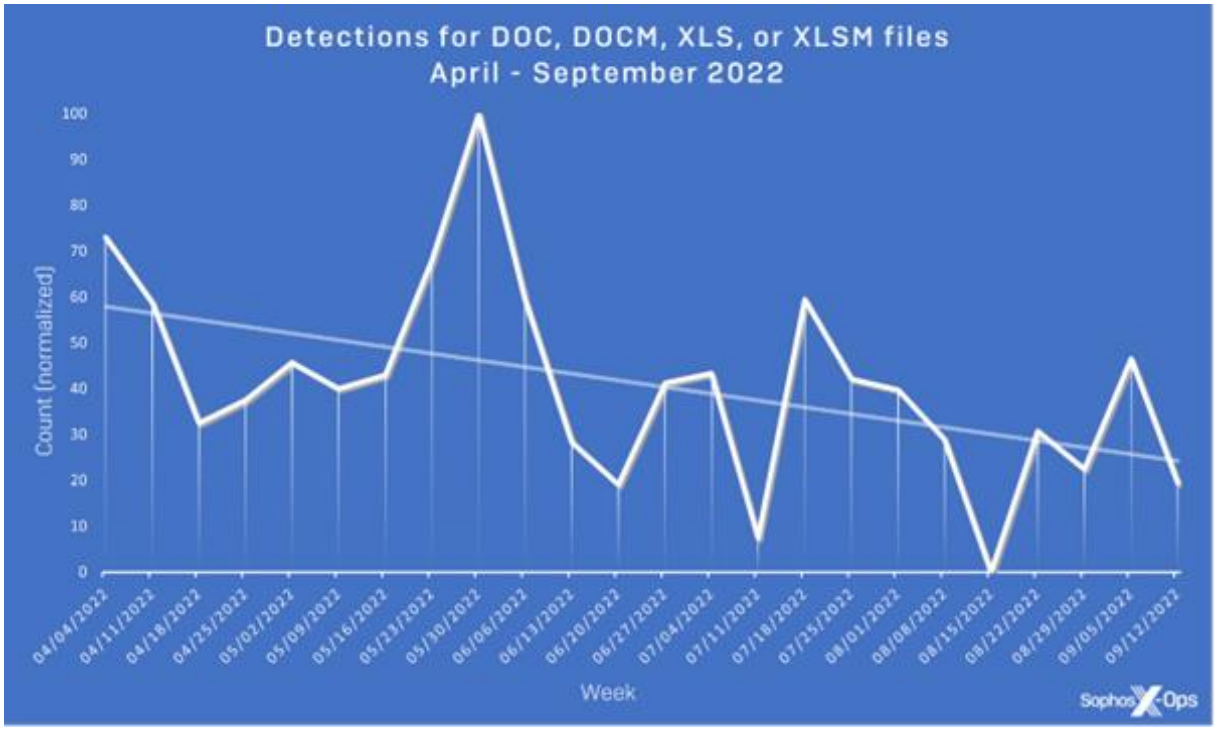
Makros sind out – Cyberkriminelle verlegen sich für die Malware-Verbreitung auf Disk-Images und Archivformate

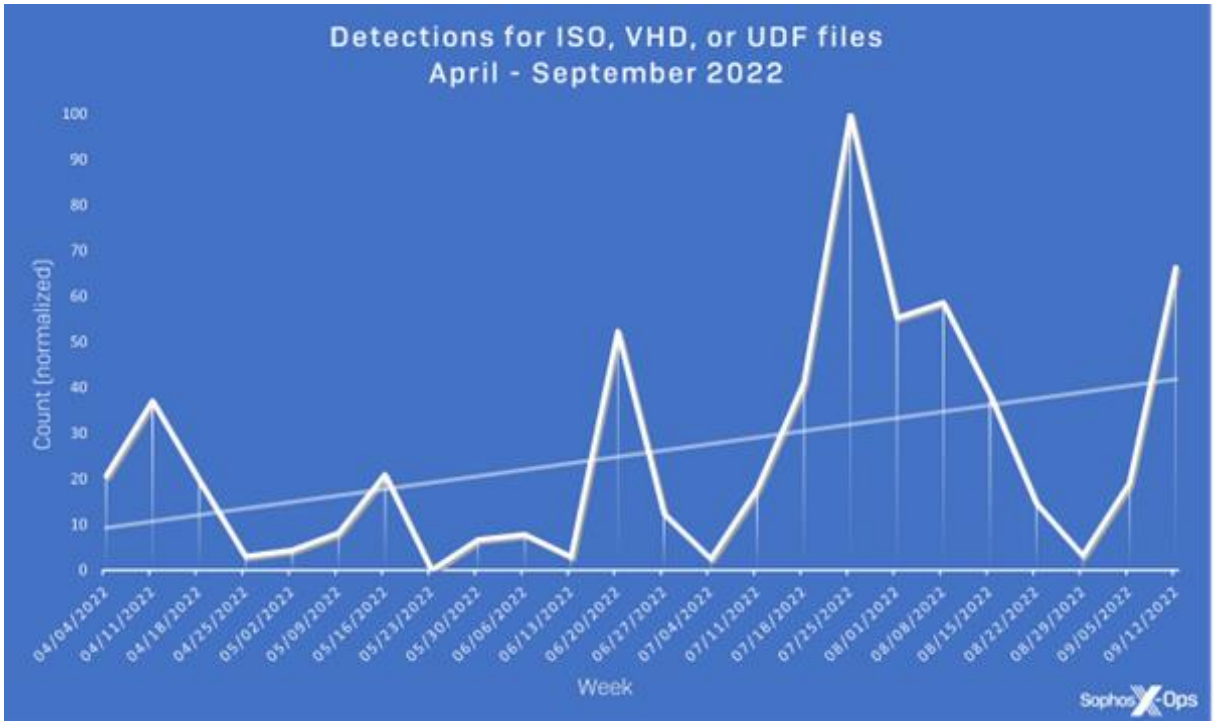
Seit der Ankündigung von Microsoft Anfang des Jahres, Makros aus dem Internet zu blockieren, zeigt sich in der Cyberkriminalität der Trend, Archiv-Formate oder Disk-Images für die Infiltration von Systemen mit Malware zu verwenden. Einfallstor Nummer eins ist dabei nach wie vor die E-Mail.

Im Februar dieses Jahres kündigte Microsoft an, dass es Makros aus dem Internet standardmäßig blockieren würde. Solche Makros werden seit Jahren von Angreifern missbraucht, um Malware zu übermitteln. Während die Sicherheits-Community spekulierte, dass Angreifer aufgrund der Entscheidung von Microsoft auf alternative Formate ausweichen würden, hat Sophos diese Tatsache anhand seiner Telemetriedaten bereits bestätigt.

Von April bis September dieses Jahres hat Sophos einen starken Rückgang der Anzahl schädlicher DOC-, DOCM-, XLS- und XLSM-Dateien festgestellt – vier beliebte Office-Formate für die Verbreitung schädlicher Makros.



Gleichzeitig war bis Mitte Juni ein stetiger Anstieg der Verwendung obskurer Archivformate (ACE, ARJ, XZ, GZ oder LZH) und ab September ein starker Anstieg der gängigeren Archivformate (ZIP, 7Z, CAB, TAR und RAR) zu verzeichnen. Auch die Verwendung von Disk-Image-Formaten (ISO, VHD und UDF) für die Verbreitung von Malware hat stetig zugenommen.



Disk-Image-Formate sind für Bedrohungsakteure besonders attraktiv, weil sie Microsofts neue "Mark of the Web"-Funktion (MOTW) umgehen. Microsoft verwendet MOTW, um festzustellen, ob ein Makro aus dem Internet stammt oder nicht; ist dies der Fall, wird es automatisch blockiert.

Sicherheitsprodukte sollten außerdem in der Lage sein, mehrere Archiv- und Disk-Image-Formate zu entpacken, darunter auch unbeliebte Formate, um diese Anhänge ordnungsgemäß auf Malware zu untersuchen. Um die Risiken weiter zu minimieren, können E-Mail-Filter so konfiguriert werden, dass bestimmte Dateiformate standardmäßig blockiert werden. Denn E-Mails zählen nach wie vor zu den Hauptangriffsvektoren.

Chester Wisniewski, Principal Research Scientist bei Sophos, sagt: "Wir geben schon seit Jahren dieselben Ratschläge für die E-Mail-Sicherheit. Dinge wie 'Klicken Sie nicht auf diesen Link' oder 'Öffnen Sie keine gefährlichen Attachments'. Die Realität ist, dass sich die Cybersicherheitslandschaft ständig verändert. Es ist unwahrscheinlich, dass Cyberkriminelle Makros vollständig aufgeben werden, denn sie passen sich mit hoher Wahrscheinlichkeit an diese neuesten Sicherheitsmaßnahmen von Microsoft an. Die Unternehmen sollten das Gleiche tun. Eine gute E-Mail-Sicherheit muss zentral verwaltet werden, wobei sich die Sicherheitsteams auf die technischen Aspekte konzentrieren, z. B. darauf, welche Dateierweiterungen gefährlich sind. Zudem gilt es die Benutzer zu schulen, wie sie vermeiden können, auf das trickreiche Social Engineering der Cyberkriminellen hereinzufallen."

Weitere Informationen über die Umstellung von Makros auf Disk-Images und Archivformate finden sich in englischer Sprache auf Sophos.com.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de