EUROPEAN-NEWS-AGENCY.COM

EUROPEAN NEWS AGENCY

International Press Service

Ressort: Special interest

Cyberstraftaten nehmen überproportional zu 05.06.2023

Göttingen, 05.06.2023 [ENA]

Es gibt viele Arten von Straftaten im Bereich der Computerkriminalität, von Jahr zu Jahr ändern sich die, ab und zu auch die Prioritäten der Straftaten. Phishing, Malware, Keylogger, Ransomware, das sind einige Begriffe, die damit zu tun haben. Schauen wir uns mal das Thema näher an.

2022 wurden im Schnitt 4.5 Millionen Euro Kosten durch Dateneinbrüche verursacht. Dabei entfielen au den Bereich Cloud 45 % aller sogenannter Data Breaches. Die hohe Zahl kommt dadurch zustande, weil inzwischen auf jedem Rechner in der einen oder anderen Form, auch auf Handys und Tablets, nicht nur beim Betriebssystem, sondern vielen Anwendungen Einzug gehalten hat. Ein Speicher, den die Benutzer bei vielen Installationen und Vertragsabschlüssen gleich kostenlos mitgeliefert bekommen; ist ja auch so praktisch – quasi von jeder Stelle, mit jedem Rechner auf seine Daten zugreifen können; das finden Hacker allerdings auch.

Einfallstore auf einen Rechner gibt es viele. Die Gründe, warum das immer noch und immer häufiger gelingt, sind vielschichtig. Menschliches Versagen, schwache Passwörter, Insiderbedrohungen, Softwareschwachstellen, Drittanbieterschwachstellen und natürlich eine Menge von Schadsoftware, die z. B. über einen Link in einer Email installiert wird, sind Gründe dafür. So hat es schon mehrfach die Deutsche Telekom betroffen, in den letzten Jahren insgesamt 8x, wenn alle Fälle bekannt worden sind. 2021 war einer der größten Fälle, betroffen waren 77 Mio. Kunden, damals wurde eine Strafe in Höhe von 350 Mio. US$ ausgesprochen.

Im Januar 2023 waren wieder 37 Mio. Kunden betroffen. Facebook, einige Kreditkartenunternehmen, der Bundestag, all das sind bekannt gewordene Firmen, Institutionen, Bereiche, wo die Hacker zuschlagen. Aber nur 10 % der Summe der erfolgreichen Angriffe werden bekannt. Denn die meisten werden nicht publik, nicht bekannt. Die Firmen haben Angst vor Kundenverlust, Reputationsverlust, Absatzeinbrüchen und damit massive wirtschaftliche Folgen. Wie schlimm die Situation geworden ist, zeigt die Straftatenstatistik: Dort hat inzwischen die Cyberkriminalität die Drogenkriminalität von Platz 1 abgelöst. Dabei haben staatlich geförderte oder unterstützte Angriffe zugenommen, insbesondere, was Russland oder China angeht.

Zum Thema Nordkorea wollte sich kein Experte auf Nachfrage äußern. Die meisten werden jetzt denken, das sind organisierte Banden, Hackerklicken und Vereinigungen, die das professionell machen. Stimmt,

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

diese Gruppe ist im Bereich der Tätergruppen auf Platz 1, aber dicht gefolgt von Privatpersonen, auch Hobbyhackern, genannt. Alle anderen Gruppen wie Konkurrenzunternehmen, Lieferanten, Beschäftigte oder Dienstleister kommen teilweise weit abgeschlagen dazu. Die Privatpersonen machen das mal aus Spaß und Hobby, einfach mal versuchen wollen und schwupps, ist man drin, die anderen versuchen zusätzlich Geld zu generieren, indem z.B. Rechnerdaten verschlüsselt werden, und weitere Motivationen mehr.

Unterstützt und leicht gemacht wird es den Privatpersonen durch Nutzbarmachung fertiger Software, die im Netz, gar nicht mal in Darknet, verfügbar sind. Ein Download ist nicht erforderlich, meist die Einzahlung eines Mitgliedsbeitrags, und schon kann die Software beauftragt werden, eine oder mehrere bestimmte Aufgaben ohne Zutun zu erledigen. Zum Beispiel sucht sie nach offenen Ports bei WLAN Kameras, bei TV Geräte, ja sogar Handys oder Drucker können ausfindig gemacht werden. Schön sortiert werden die Ergebnisse nach Land, Stadt, Firma und dann mit Gerätenahmen sortiert, dann die offenen Ports angezeigt, und der Privatnutzer kann ohne Kenntnisse einfach per Mausklick den Port benutzen, um in das System einzudringen.

Und das man damit einige lustige Dinge bewerkstelligen kann, die trotzdem nicht in Ordnung sind, zeigt ein Test, der mir informativ nachträglich von einem Hobbyhacker zugänglich gemacht wurde. Da wurden auf einem Privathandy die gespeicherten Videos und Fotos angeschaut, da wurde in einem Vorgarten eines Privathauses der Swimmingpool und das Treiben über die installierte Sicherheitskamera eingesehen oder in einer Firma Druckerdaten wie Füllstände der Patronen, Seriennummer und andere technische Details abgerufen. Die aufgezählten Beispiele berufen sich auf nachträgliche Erzählungen der Person.

Was kann getan werden ? Privat natürlich eine Firewall, ein verschlüsseltes WLAN – Netz und Virusprogramm installiert haben, dazu in regelmäßigen Abständen Softwareupdates suchen und installieren und bei „ seltsamen „ Rechnerproblemen die kompletten Festplatte(n) nach Schadsoftware durchsuchen. Und in regelmäßigen Abständen Sicherheitskopien erstellen, am besten die Festpatte spiegeln.
Bei Firmen gilt im Prinzip das Gleiche in großen Stil, hier ist der Faktor Mensch dazu ein bedeutender Faktor.

Regelmäßige Schulungen und Vermittlung von neuen Bedrohungsarten, Umgang mit „ unbekannten „ Email Absendern oder auch bekannten Absendern, die etwas aussergewöhnliches verlangen. Lieber einmal mehr fragen als einmal mehr falsch klicken. Denn die Hacker entwickeln sich mit der vorhandenen Technik, Software und immer neuen Möglichkeiten wie die KI Technologie weiter; die Sicherheitsbeauftragten können selten einen Schritt voraus sein, sondern immer nur möglichst schnell nachziehen. Denn wie soll ein Sicherheitsbeauftragter eine neue Bedrohung bekämpfen oder abschalten, wenn er die noch gar nicht kennt ?

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

Eine recht neue Art der Datensicherheit ist der Einsatz von Tokens. Dabei werden Klartextdaten durch Tokens ersetzt, nicht verschlüsselt. Daher gibt es beim Einsatz von Tokens auch keinen Schlüssel zur „ Entschlüsselung „, sondern das Ganze basiert auf einem Rechensystem. Das Motto dieser neuen derzeit sicheren Art des Datenschutzes: Tokens enthalten die Nutzbarkeit von Geschäftsprozessen und Analysen. Mit Tokens werden die Daten sicher und nutzbar. Na dann.

Dem Bericht angehängt habe ich 6 Screenshots. 3 davon sind typische Fake Emails mit den üblichen Möglichkeiten sich ein Problem einzufangen. Dabei sind Fake-Emails häufig zu erkennen: Schlechtes Deutsch, fehlende Grafiken der benutzten Firma, eine seltsame Absender – Email oder der Anhang im ZIP – Format. Häufig wird von einer angeblichen Bestellung, einer Sendeverfolgung eines Pakets oder einer Bankdatenverifizierung gesprochen. Die 3 anderen Screenshot zeigen ein Beispiel wie ein Hackertool arbeitet, um Schwachstellen im System zu finden.

Natürlich wurden auf den Screens relevante Daten, Firmennamen usw. gelöscht oder unkenntlich gemacht. Bei den Emals kann man häufig schon am Absender erkennen, das hier was nicht stimmt. Und die Verwendung der Crawler - Software alleine schon deshalb nicht unbedenklich, weil Sie und andere auch den Hersteller nicht kennen. Was sammelt er über Sie während Sie die Software nutzen ? Das weiß keiner. Quelle: Teile der statistischen Informationen wurden aus dem Webinar der Firma Comforte AG, einer Datensicherheitsfirma, mit dem Titel Cybersecurity 2023, präsentiert vom CEO Herrn Michael Deissner, als Gedächtnisprotokoll verwendet. Mehr Informationen zu der Firma Comforte unter: www.comforte.com .

Bericht online lesen:
https://www.european-news-agency.de/special_interest/cyberstraftaten_nehmen_ueberproportional_zu_05062023-86596/

Redaktion und Verantwortlichkeit:
V.i.S.d.P. und gem. § 6 MDStV: Uwe Hildebrandt

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

Von LandesBank Berlin A.G <contato+clientes@nuvemshop.com.br>

An Mich <

Antwort an mario-pedrikshdgs@hotmail.com

Betreff **Re: [LBB.DE] : Benachrichtigung wichtig !.**

Antworten | Weiterleiten | Archivieren | Junk | Löschen | Mehr

07:58

Ihre LBB-karte wurde aus Sicherheitsgründen gesperrt. Bitte bestätigen Sie Ihre Identität so schnell wie möglich, um sie zu entsperren. Wir benötigen Ihre Hilfe, um alle Ihre Bankkontodaten zu überprüfen. Dieser Vorgang dauert 5-10 Minuten und danach können Sie Ihr Konto entsperren.

Entsperren Sie Ihr Konto

TOTAL RESULTS

228,293

TOP COUNTRIES

China	158,278
United States	15,275
Korea, Republic of	9,625
France	4,879
Germany	4,239

More...

TOP PORTS

515	27,001
445	26,838
5353	8,403
631	7,481
161	1,118

More...

TOP ORGANIZATIONS

Aliyun Computing Co., LTD	125,190
Aliyun Computing Co.LTD	9,215
Korea Telecom	7,076
China Mobile Communications Corporation	6,640
Hangzhou Alibaba Advertising Co.,Ltd.	2,006

More...

TOP PRODUCTS

Samba	13,811
mDNS	8,403
CUPS (IPP)	7,584
RICOH Co. Ltd.	904
Microsoft RPC	155

More...

TOP OPERATING SYSTEMS

Windows 6.1	10,743
Unix	3,066
Windows 7 Professional 7600	836
Windows 5.1	465
Windows Server 2012 R2 Standard 9600	447

More...

186.·

182.· anycast.cnt-gr
ms.ec
CORPORACION

Ecuador, Quito

```
SMB Status:
  Authentication:
  SMB Version: 1
  OS: Windows 6.1
  Software: Samba 4.7.6-Ubuntu
  Capabilities: dfs, extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-read, nt-find, nt-smb, nt-status, raw-mode, rpc-remote-api,

Shares
Name                 Type       Comments
---------------------------------------------------------------------------
print$               Disk       Printer Drivers
IPC$                 IPC        IPC Service (terminalquevedo server (Samba, Ubuntu))
manam7               Printer    mana oficina 8
manag10              Printer    mana oficina 10
buenafeqvd           Printer    EPSON TMT88V
quevedo41            Printer    QUEVEDO CONSROCIO
bol38                Printer    bol38
sucreg19             Printer    sucre venta gye
panamericana27       Printer    oficina 27 panamericana
putumayo9            Printer    Oficina 9
ambato15             Printer    oficina 13
quevedo21            ...
```

186. [redacted]

// TAGS: database self-signed

// LAST SEEN:

General Information

Hostnames	**182.**	**anycast.cnt-grms.ec**
Domains	CNT.	
Country	**Ecuador**	
City	**Quito**	
Organization	**CORPORACION**	
ISP	**CORPORACION**	
ASN	**AS28**	

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2019 A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

Open Ports

22 80 137 445 631 3306 10000

// 22 / TCP

-44025763 |

OpenSSH 7.6p1 Ubuntu-4ubuntu0.5

```
H-2.0-OpenSSH_7.6p1 Ubunt  4ubuntu0.5
   type: ssh-rsa
Ke  AAAAB   yc2EAA  ABAA  BtKRM6T  +iT7  6xw  e0eO5/6tw06gKoGH
N6J  L  +E  AY  NDhk1AD/  R  iO5T3tt5A  +0WYQYrC41npi4
uMmsA  X96TJ/9  qq38gK60Uyfr  ZoXY0hg7gNyQ  YHT3Eo8F86S6+
YYP  PA7LSF  6JIUob9  5urFHFIbi/  oTSed  Vn6DAvnUCb
  o7aDi  tyH  j  7  yWXDEF/  8kTSP  akMU1wsZAv
ingerprint  d:91:  :53:90:29:22:2e.  6:  d:d8:94

Kex Algorithms:
        rve25519-sha256
         e25519-sha256@libssh
      ec  ha2-nistp256
      ecdh  2-nistp384
      ecdh-s  istp5
      diffie-h  oup-exchange-sha256
      diffie-he  roup16-sha512
      diffi  ma  n18-sha512
      d  ellman-gr  sha256
        rie-hellman-group1

Server Host Key Algorithms:
        h-rsa
        ha2-512
      rsa-
      er  tp256
          ed25519
```

Password changed Facebook 18:01

Von Facebook <info@utilitical.com>

An h395@yahoo.com 18:01

Betreff **Password changed**

Antworten | Allen antworten | Weiterleiten | Archivieren | Junk | Löschen | Mehr

Thunderbird hat diese Nachricht als Junk eingestuft. Weitere Informationen | Kein Junk

Your Facebook password was changed on Fri,30 Dec-2022,

Operating system : Windows

Browser : Chrome

IP address : 192

Estimated location: Los Angeles, California, US

If you did this, you can safely disregard this email.

If you didn't do this, please click here to secure your account

Report the user Yes, me

Thanks,
The Facebook Security Team

This message was sent to If you receive this message in your junk mail, mark it as ' not spam ', to click to confirm or Report
Facebook, Inc., Attention: Community Support, 1 Facebook Way, Menlo Park, CA 94025

To help keep your account secure, please don't forward this email. Learn more. ;

Vergütung • Office File 01.06.2022, 18:18

Von Office File <solomonkibler635@gmail.com>
Betreff **Vergütung**
Antwort an agentesternunion9@yandex.com
An undisclosed-recipients:;
Blindkopie (BCC) Mich <

Antworten | Weiterleiten | Archivieren | Löschen | Mehr

01.06.2022, 18:18

Thunderbird hat diese Nachricht als Junk eingestuft. Weitere Informationen | Kein Junk

Vergütung

U.S $4,000 ZAHLUNG SCHICKTEN WIR HEUTE ABHOLEN.

Der IWF entschädigt alle E-Mail-Adresse, das war Fonds als einer der ward win Opfer und Ihre mail-Adresse und Ihr name ist eine der genehmigten Summe von $3.7 Millionen US-DOLLAR zu zahlen aufgeführt. Wir haben abgeschlossen, um Ihre eigene Zahlung durch Western Union Geldüberweisung zu bewirken, um diese Fonds in gutem Zustand zu Holen, $4,000 zweimal täglich, bis die Gesamtsumme von $3,7 Millionen usd vollständig an Sie übertragen wird. Wir brauchen jetzt Ihre Informationen, wo wir die Mittel senden werden, wie; Empfängername(Ihr voller Name) Adresse und Telefonnummer. Kontaktieren Sie Western Union mit dieser E-mail: (agentesternunion9@yandex.com) mit Ihren vollständigen Informationen. Für dringende Anfrage rufen Sie Herrn Paul Williams +229 61167883 für die Zahlung.

Herr Paul Williams
Telefon: +229-61167883
E-mail :(agentesternunion9@yandex.com)

Rufen Sie Mr. Paul Williams sofort erhalten Sie diese E-mail, damit er Ihre Zahlung sofort beschleunigen, um die $4000 dollar MTCN an Sie für Ihre Abholung der Zahlung OK freigegeben.

(1)Ihr Vollständiger name:
(2)Ihre Telefonnummer:
(3)Ihr Land:
(4)Ihr Alter:

Danke,

Frau Susan Ude
Kontaktieren Sie Dir. Western Union Überweisung,
Cotonou, Benin Republic