



Super Bowl: Sport-Fans landeten auf infizierten Websites
 von Markus Pilzweiger
 05.02.2007, 15:36
 Der Super Bowl sorgt in den USA alljährlich für Ausnahmezustand. Im Vorfeld der Sportveranstaltung erleben auch Websites, die sich mit dem Thema Football beschäftigen, einen wahren Höhenflug. Ein Umstand, den sich Hacker zunutze gemacht haben, um ihre Malware unters Volk zu bringen.
 Im Vorfeld des diesjährigen Super Bowl haben Sicherheitsexperten entdeckt, dass die Websites des "Dolphin Stadium" und des Football Teams "Miami Dolphins" offenbar gehackt und...

Auf einer bekannten US-Webseite konnten User sich über die Superbowls Games in Miami informieren und online Tickets bestellen – was sie nicht bemerkten: Allein durch den Besuch der Webseite wurde ein Malware-Download auf ihren PC aktiviert.



Datenraub schreckt Jobportale
 Betreiber von Internetplattformen verschärfen Sicherheitsmaßnahmen nach Angriff auf Monster.com
 VON STEPHAN RADOMSKY, HAMBURG
 Der Datenverlust beim weltgrößten Jobportal Monster.com hat in der Branche für einige Aufregung gesorgt. Anbieter ähnlicher Dienste reagierten nervös auf die Nachricht vom Diebstahl von Daten.
 Unternehmen am Freitag mit. Bereits am Dienstagabend hatte die Sicherheitsfirma Symantec gemeldet, dass Monster-Nutzer von einem Virus bedroht seien – was sich später nach Angaben von Monster als falsch herausstellte. Richtig war, dass ein sogenannter Trojaner in die Computer-Systeme eingedrungen war und Daten für die...

Über 1,3mio Lebensläufe wurden mittels eines Trojaners von einem weltweit bekannten Jobportal entwendet und als Basis für Phishingangriffe genutzt – Ziel waren die Bankdaten der User.

„WEB THREATS“

DIE BEDROHUNG, DIE AUS DEM INTERNET KOMMT

Das Bedrohungsszenario für Unternehmen verändert sich derzeit: Kam bisher noch die überwiegende Anzahl der Attacken per eMail, so nimmt der Anteil der webbasierten Angriffe rapide zu und wird 2008 die Mehrheit der täglichen Abwehrarbeit beanspruchen.

Die richtige Strategie für den Schutz Ihres Unternehmens entwickeln zu können, setzt voraus, dass Sie die „Web Threats“, ihre Funktionsweisen und Hintergründe kennen und wissen, welche Lösungsansätze zu welchen Ergebnissen führen.

Wir wollen Ihnen daher im Folgenden einen schnellen und kompakten Überblick über das Thema geben, damit Sie unseren Wissensvorsprung zu Ihrem Produktivitätsgewinn machen können.

WAS SIND „WEB THREATS“?

Grundsätzlich bezeichnet man als „Web Threats“ sämtliche Bedrohungen, die webbasiert sind und entweder vom User selbst durch den Besuch einer Webseite oder von bösartigen Applikationen direkt in Gang gesetzt werden.

Entscheidend sind folgende Unterschiede zu bisherigen Threats:

- Nicht mehr um große Aufmerksamkeit zu erreichen, sondern im Verborgenen
- Nicht mehr global, sondern regional bis lokal
- Nicht mehr ungerichtet breit streuend, sondern zielgerichtet, oft auch zielgruppenorientiert
- Nicht mehr einmalig, sondern sich wiederholend
- Nicht mehr eindeutig bestimmbar, sondern sich permanent verändernd

Die explodierende Zunahme neuer und wechselnder Domains bringt herkömmliches URL-Filtering und Scanning Technologien an ihre Grenzen und stellt die strukturelle Basis für die „Web Threats“

dar. Es werden verschiedene, über eMail- oder Web-verbreitete Angriffe kombiniert, die weitere Teile aus dem Internet herunterladen, welche sie dann zu einem Trojaner oder Keylogger selbstständig zusammenbauen und nach Bedarf auch verändern. Das Ganze passiert ohne Wissen und Zutun des Anwenders. Die Infektion erfolgt immer öfter durch Aufruf einer manipulierten Webseite, wobei es sich oft um vertrauenswürdige Web-Angebote handelt, die von Hackern unbemerkt zweckentfremdet wurden.

Diese unterschiedlichen Angriffe, die von der Webseite mit „nur“ einem bösartigen Code bis zur komplett manipulierten „Webseiten-Attrappe“ reichen, haben in ihrer Konsequenz massive Auswirkungen:

Wenn Webseiten nicht mehr das sind, was sie zu sein scheinen, wird der früher ungefährliche Besuch von Webseiten (also das klassische „Surfen“) zum Risiko für jedes Unternehmen und jede Privatperson.

WIE FUNKTIONIEREN „WEB THREATS“?

Der „Erfolg“ der „Web Threats“ hat verschiedene Ursachen:

Die zunehmende und immer globaler werdende Web 2.0-Popularität vervielfacht die Kommunikationsmöglichkeiten zwischen den Menschen. Kombiniert mit dem Ansatz des „Social Engineering“, also dem Ausnutzen menschlicher Eigenschaften, wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität, zur Erlangung geheimer Informationen, eröffnet eine Vielzahl unterschiedlichster Angriffsmöglichkeiten.

Technisch erleichtert werden diese durch den Umstand, dass der Internet-Port 80 fast ständig offen ist. Schließlich wird nur so gewährleistet, dass Mitarbeiter die Produktivitätschancen des Internet dank seiner Informationsfülle und Kommunikationsmöglichkeiten auch umsetzen können.

Die Unternehmen stehen daher vor einem schier unlösbaren Problem:

Während sie den eMail-Verkehr weitestgehend schützen können, ist der in real time stattfindende Webtraffic mit den bisher verfügbaren Mitteln nur schwer zu kontrollieren. Die Folge sind u. a. mehr als 500 Millionen mit einem Trojaner infizierte PCs im Jahr 2006. Dabei geht es nicht nur um das Ausspionieren privater Onlinebanking- und geheimer Unternehmensinformationen, sondern oft genug auch um die „feindliche Übernahme“ des PCs, um ihn z. B. als Teil eines peer-to-peer kontrollierten Botnets für weitere Malware-Aktivitäten einzusetzen.

Letzteres wiederum führt dazu, dass ein User von einer vermeintlich glaubwürdigen Quelle kontaktiert wird und entsprechend leichtgläubig handelt.

Zusätzlich stellt die Taktik einer Infektion auf regionaler und lokaler Ebene, die nicht die Technik der Masseninfizierung früherer Malware-Vorgehensweisen verwendet, eine neue Dimension der Bedrohung dar.

Die Infektionskette

AUSGANGSPUNKT	INFEKTIONSROUTINE	PAYLOAD
<ul style="list-style-type: none"> • Anwender klickt auf manipulierte URL in einer eMail oder Instant Message • Anwender wird über einen infizierten DNS, eine gefälschte Webseite oder manipulierte Suchergebnisse an eine bösartige URL weitergeleitet. • Anwender lädt Software/Freeware herunter, die unsichtbar mit Malware verknüpft ist • Anwender lädt scheinbar gutartige Mediendateien herunter (Bilder, Videos, Musik, Animationen), hinter denen sich Malware verbirgt 	<ul style="list-style-type: none"> • Installierte Anwendungen laden weitere bösartige Anwendungen/Programme herunter und installieren sie • Automatisches Update über das Web durch Download von Teilen des Update-Code zur Vermeidung einer Entdeckung 	<ul style="list-style-type: none"> • Spyware/Grayware, die Daten/Informationen vom System stiehlt und an Dritte versendet • Adware/Data Miner/Pop-up zu kommerziellen Zwecken • Browser Helper Objects verfälschen Suchmaschinenergebnisse oder verfolgen das Surfverhalten, um unerwünschte Werbung zu platzieren • Von Dritten kontrollierte Bots oder Zombies

WELCHE ZIELE VERFOLGEN DIE ANGREIFER?

Ob es sich um infizierte Webseiten, manipulierte Suchergebnisse oder täuschend echt nachgebaute „Webseiten-Attrappen“ handelt - das Ziel dieser Angriffe ist immer das gleiche: Geld.

Professionell aufgebaute, kriminelle Organisationen, die zumeist weltweit operieren, haben das enorme Potenzial des World Wide Web erkannt und setzen inzwischen mit dem Diebstahl persönlicher und Unternehmensinformationen Milliarden um.

Das Internet hat als Dreh- und Angelpunkt aller kriminellen Aktivitäten eine Untergrund-Ökonomie geschaffen, die von der Einmalzahlung für die Entwicklung bzw. Bereitstellung von Malware-Komponenten bis hin zur regelmäßigen „pay-per-download“-Abrechnung verschiedene Business-Modelle reicht.

Wer übrigens meint, dass Privater mit ihren Bankdaten im Fokus der Verbrecher stünden, irrt gewaltig: Die Anzahl der virtuellen Wirtschaftsspionage-Fälle erreicht „dank“ der Möglichkeiten der

„Web Threats“ traurige Rekordhöhen - und trifft Unternehmen jeder Größe und nahezu jeder Branche.

Die Untergrund-Ökonomie

EINE AUSWAHL VON PRODUKTEN, DIE IN TYPISCHEN CYBERCRIME-FORUMS VERKAUFT WERDEN:	
\$ 1000-5000	Trojaner zum Stehlen der Informationen zu Online-Accounts
\$ 500	Kreditkartennummer mit PIN
\$ 80-300	Veränderung von Rechnungsdaten einschließlich Kontonummer, Rechnungsadresse, Sozialversicherungsnummer, Name, Adresse und Geburtsdatum
\$ 150	Führerscheinnummer
\$ 150	Geburtsurkunde
\$ 100	Sozialversicherungskarte
\$ 7-25	Kreditkartennummer mit Sicherheitscode und Ablaufdatum
\$ 7	Paypal-Benutzername und Passwort

WELCHE GEGENMASSNAHMEN GIBT ES?

Scan-basierte Lösungen bilden zwar das Rückgrat der Unternehmenssicherheit, aber allein sind sie den modernen „Web Threats“ nicht gewachsen. Da diese aus verschiedenen Komponenten bestehen, muss auch die Abwehr mehrschichtig sein.

Benötigt werden also Lösungsansätze, die unterschiedlichste Informationsquellen intelligent in Beziehung setzen, um „Web Threats“ zu identifizieren. Dabei muss die Sicherheitstechnologie sowohl auf Desktops und Gateways präsent sein als auch in Echtzeit im Internet.

Konsequenterweise muss jede sinnvolle Abwehrstrategie folgende Bestandteile enthalten:

- Dynamische Web Reputation
- URL-Filtering (Blacklisting)
- Domain-Profilung
- eMail-Security - Phishing- & Spam-Correlation (eMail-Reputation)
- Content Scanning (am Gateway und am „Endpunkt“ = Server, PC, Laptop)

Nur mit einer Kombination der oben genannten Einzelmaßnahmen kann ein Unternehmen seine Mitarbeiter und seine Werte adäquat schützen – eine Investition, die sich schnell bezahlt macht.

„TOTAL WEB THREAT PROTECTION“ - DIE LÖSUNG VON TREND MICRO™

„Total Web Threat Protection“ ist eine mehrschichtige, umfassende Abwehrstrategie, die gleichzeitig an den neuralgischen Punkten ansetzt:

- Internet (in-the-cloud)
- Gateway
- Endpoint (PC, Laptop)

„Total Web Threat Protection“ ergänzt die bewährten Funktionen für Client- bzw. Server-Sicherheit und verknüpft umfangreiche Datenquellen, wie beispielsweise Domain- und URL-Historie, IP-Location und eMail-Reputation, wodurch sich „Web Threats“ mit großer Genauigkeit identifizieren lassen. Wenn ein Trend Micro™ Anwender eine neue URL aufruft, wird die Webseite von der mehrstufigen „Total Web Threat Protection“ sofort analysiert und die Datenbank nahezu in Echtzeit aktualisiert – damit sind weltweit alle Anwender sofort geschützt.

Darüber hinaus kontrolliert „Total Web Threat Protection“ Verbindungsanfragen, die von im Hintergrund laufenden Prozessen gestellt werden: Versucht also ein Spionageprogramm, die gesammelten Daten über das Internet zu versenden oder eine

neue Malware-Komponente herunterzuladen, wird die Ziel-Adresse in Echtzeit analysiert und auf Unbedenklichkeit untersucht. Treten dabei Verdachtsmomente auf, blockiert „Total Web Threat Protection“ die Verbindung. Im Gegensatz zu Personal Firewalls lässt sich „Total Web Threat Protection“ also auch durch die Verwendung häufig genutzter Standard-Ports (z. B. 80 für HTTP) nicht täuschen und ermöglicht eine intelligente Sicherheitsbewertung der Empfangsadresse.

Webseiten und eMails, die Malware verbreiten, lassen sich daher mit „Total Web Threat Protection“ bereits an den Grenzen des Netzwerks blockieren, Malware-Infektionszyklen werden unterbrochen und der Versand gestohlener Daten wird verhindert. Durch die Bereitstellung der „Total Web Threat Protection“ über das Internet reduziert sich die Belastung von IT-Ressourcen und Bandbreiten, wovon insbesondere mittelständische Unternehmen und mobile Anwender profitieren.

Zusammengefasst wird mit „Total Web Threat Protection“ eine Aktualität der Sicherheitsmaßnahmen erzielt, die mit dem bisherigen Zyklus von Malware-Entdeckung, Pattern-Generierung und -Verteilung kaum möglich wäre.

DIE VORTEILE EINES WELTUMSPANNENDEN SICHERHEITSNETZES

Die TrendLabs untersuchen Hunderte von Millionen von Webseiten auf ihr Alter, ihre Herkunft, ihre Historie und alle Aktivitäten, die von diesen ausgehen, also z. B. Mails oder andere Applikationen. Damit entstehen umfangreiche Datenbanken mit vollständigen Profilen von bekannten, verdächtigen und auch potenziellen, künftigen Angreifern.

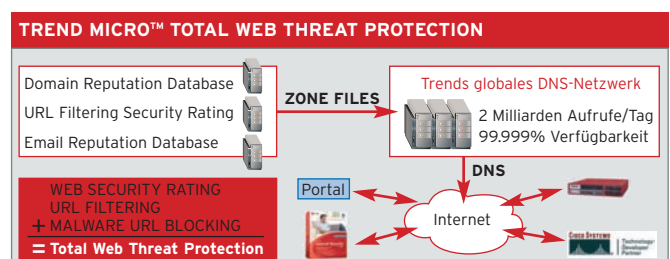
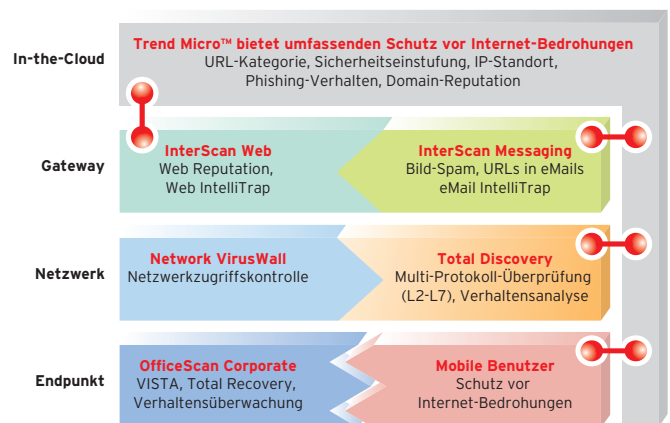
Diese Informationen werden permanent durch Daten und Hinweise aus aller Welt aktualisiert (**derzeit 2,5 Milliarden Anfragen pro Tag!**) und bei jedem Verbindungswunsch in Echtzeit abgefragt.

Mit diesem URL-Rating erhält der User drei Möglichkeiten:

- Freigabe für den problemlosen Empfang einer Mail oder den Besuch einer Webseite
- Hinweis auf evtl. Unsicherheiten einer Webseite oder Mail
- Zugriffsverweigerung aufgrund der erkannten Gefahr

Da jeder User von Trend Micro™ Produkten Teil des weltweiten Sicherheitsnetzes ist, kommen dessen Vorteile JEDEM User zugute. So kann der Aufruf einer neuen/unbekannten infizierten Webseite durch einen User in Asien dazu führen, dass ein Unternehmen in Europa schon 15 Minuten später davor geschützt ist, dieselbe Webseite zu besuchen.

Auf diese Weise entsteht eine einzigartige, gemeinschaftliche Intelligenz, die in der Lage ist, die „Web Threats“ kraftvoll und konsequent abzuwehren.



DIE VORTEILE VON „TOTAL WEB THREAT PROTECTION“

„Total Web Threat Protection“ vereint Anti-Virus, Anti-Spyware, Anti-Phishing, Anti-Spam mit Web Reputation, URL-Filtering und HTTP-Traffic-Scanning - und ist somit auf die Heterogenität der Angriffe vorbereitet.

Sie ist dynamisch, da sie in Echtzeit die Reputation einer Quelle analysiert und darauf reagiert - sie arbeitet integriert, denn sie koordiniert die Abwehr, die Beseitigung der Malware und die Wiederherstellung der angegriffenen Daten.

Die Vorteile im Überblick:

- **Up-to-date:** im Gegensatz zur lokalen Datenbank bietet die Onlineabfrage ständig aktuelle Werte
- **Schnell:** kürzere Zugriffszeiten gegenüber lokaler Datenbank
- **Leistungsstark:** kein Updatetraffic
- **Umfassend:** richtet sich nicht nur gegen Würmer, Viren u. ä., sondern auch und gerade gegen Bedrohungsszenarien, wie Phishing, Pharming etc.
- **Einfaches Handling:** Wahlfreiheit des Sicherheitslevels ermöglicht Unterscheidung zwischen „known good“, „known bad“ und diversen Zwischenstufen
- **Intelligent:** Der Administrator definiert Art und Menge der verwendeten Informationen
- **Effizient:** Blockade der Quelle statt Beseitigung der Symptome
- **Sicher:** legitime Webinhalte werden durchgelassen, problematische geblockt

Best Practices für Ihre Web Sicherheit

NUTZEN SIE WEB THREAT PROTECTION, UM WEB THREATS ZU BLOCKIEREN, BEVOR SIE DAS NETZWERK INFILTRIEREN
Für Mitarbeiter inner-/außerhalb des Unternehmensnetzwerks

NUTZEN SIE HTTP MALWARE UND ANTI-SPYWARE SCANNING
Mitarbeiter müssen alle Webanfragen an den Scanner senden

GEWÄHREN SIE UNNÖTIGEN PROTOKOLLEN KEINEN ZUGRIFF ZU IHREM UNTERNEHMENSNETZWERK
P2P und IRC sind extrem gefährlich, da sie überwiegend von Botnets benutzt werden

SETZEN SIE IN IHREM NETZWERK „VULNERABILITY SCANNER“ EIN
Halten Sie Betriebssystem und andere Anwendungspatches stets auf aktuellstem Stand

SCHRÄNKEN SIE DIE BENUTZERRECHTE ALLER NETZWERKNUTZER EIN
Gewähren Sie nur wenigen Anwendern Administrator-Rechte

UNTERSTÜTZEN SIE KAMPAGNEN ZUR SENSIBILISIERUNG DER USER
Zeigen Sie Ihren Mitarbeitern die Gefahren bei der Nutzung von Netzwerken an Flughäfen, in Cafés, zu Hause usw. auf

Für mehr Informationen erreichen Sie uns telefonisch unter
D: 0800 330 4533, A: 0800 880 903, CH: 0800 330 453
oder per eMail sales_info@trendmicro.de.

Gerne stellen wir Ihnen kostenlos weiteres Informationsmaterial zur Verfügung.

WARUM „WEB THREATS“ EINE CHANCE FÜR UNTERNEHMEN SIND

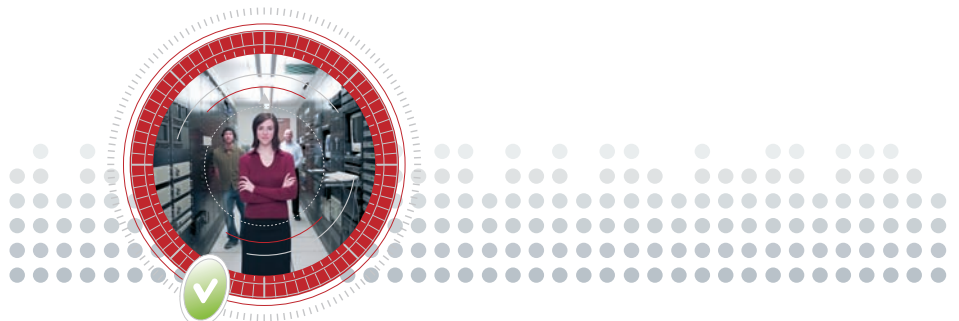
Selbstverständlich weiß niemand, wann der nächste Fall eines „Web Threats“ auftreten kann bzw. ob einer Ihrer Mitarbeiter aus Versehen auf eine infizierte Webseite geht.

Doch unserer Meinung nach liegt im frühen Einsatz der „Total Web Threat Protection“-Lösungen eine große Chance für Unternehmen, ihre IT-Infrastruktur zu stärken und ihre Ressourcen von sicherheitsrelevanten Aufgaben zu entlasten. Zudem haben zahlreiche Studien eindeutig belegt, dass die Kosten und der Zeitaufwand NACH einem Angriff die Implementierungskosten einer Abwehrlösung um ein Vielfaches übersteigen.

Für Sie als Unternehmen bedeutet dies, dass Sie sich unseren Innovationsvorsprung zunutze machen und in einen Effizienzvorsprung für Ihr Unternehmen verwandeln können. Denn wenn Sie Ihr Unternehmen schon heute auf die „Web Threats“ vorbereiten, sichern Sie im Falle eines erfolgreich abgewehrten Angriffs die Produktivität Ihrer Mitarbeiter und damit die Werte Ihres Unternehmens.

www.trendmicro-community.com

D: 0800 330 4533
A: 0800 880 903
CH: 0800 330 453



Trend Micro™ Deutschland GmbH
Central Europe
www.trendmicro-europe.com

Lise-Meitner-Straße 4
85716 Unterschleißheim

Tel.: +49 (0) 89 37479-700
Fax: +49 (0) 89 37479-799



Securing Your Web World