GreenPoint>
Legal

GAME NOT YET OVER FOR BANK FRAUD MALWARE

In 2009, the FBI began investigating a Russian hacker known as "lucky12345" on suspicion of creating the malicious software dubbed "Zeus," which was allegedly used by his cyber-gang to steal victims' passwords, bank account information and other sensitive personal data. In 2011, the malware was "upgraded" and renamed "Gameover Zeus" (GOZ). After more than 1 million infections globally and financial losses in the hundreds of millions of dollars, authorities have identified the criminal mastermind. But the game isn't over yet.

Cyber-Racketeering

GOZ malware is spread via spam and phishing emails that link the unsuspecting end-user to compromised websites after which the cyber-criminals are able to access — and often empty out — victims' online bank accounts. One particularly sneaky feature of GOZ is that it can lay dormant on a computer until it detects just the right opportunity to wake up and cause its harm. At that point, it sends critical account access information back to the criminals' network allowing them to drain the bank account.

Cyber-Ransom: One Bitcoin

If GOZ determines that the system where it resides is not that of a "viable" victim, it then turns on a lock-down mode that freezes data — from photographs and music to personal files — until the user pays a ransom to unlock it. In one reported case, a U.S. police force was forced to pay a ransom in order to get its files released. The ransom was one bitcoin, untraceable as a crypto-currency, unlike dollars or other legal tender.

Criminal Charges Filed

In 2012, the United States indicted the hacker under his screen name "lucky12345" in federal district court in Nebraska on charges of bank fraud, conspiracy to violate the Computer Fraud and Abuse Act and aggravated identity theft. This past May, after the 30-year-old Russian's true identity was uncovered, he was indicted in the Western District of Pennsylvania for conspiracy, computer fraud, wire fraud, bank fraud and money laundering. On May 30, a complaint was filed in district court in Nebraska tying the "lucky12345" charges to the named defendant. His network is said to include cohorts in the Ukraine and the UK — as evidenced by over 15,000 infections of British computers. The legal challenges for both the United States and the UK are exacerbated by the fact that Russia does not extradite criminal defendants for foreign prosecution.

Technical Stop-Gaps

Although global law enforcement agencies have been able to counterattack the control servers hosting GOZ, they caution that the fix may not be permanent: It is believed that a mere two-week respite exists before the cyber-criminals rebuild their network. During that period, cyber-crime experts recommend that users install and update — to the latest version — anti-virus software.

CONTACT US

DAVID T. KINNEAR
O: 212.913.0500 x565
M: 917.886.3222
E: DAVID.KINNEAR@GREENPOINTGLOBAL.COM

WILLIAM H. ANDERSON, ESQ
O: 212.913.0500 x586
M: 914.672.4975
E: WILLIAM.ANDERSON@GREENPOINTGLOBAL.COM

WWW.GREENPOINTLEGAL.COM