USSR's old domain name attracts cybercriminals

May 31 2013, by Raphael Satter

Sergei Ovcharenko, the director for .su domain development at Moscow's Foundation for Internet Development smiles as he speaks to The Associated Press photographer in his office in Moscow, Russia, on Thursday, May 30, 2013. The Foundation for Internet Development is responsible for managing the Soviet Union's old .su domain, which security experts say has become a magnet for hackers. Ovcharenko acknowledges that criminal sites hosted in Soviet cyberspace can stay online for extremely long periods of time, something he blames on weak Russian legislation and outdated terms of service. He promises that stricter rules are on their way. (AP Photo/Alexander Zemlianichenko)

The Soviet Union disappeared from the map more than two decades ago. But online an 'e-vil empire' is thriving. Security experts say the .su Internet suffix assigned to the USSR in 1990 has turned into a haven for hackers who've flocked to the defunct superpower's domain space to send spam and steal money.

Capitalist concerns, rather than Communist nostalgia, explain the move.

"I don't think that this is really a political thing," Oren David, a manager at security firm RSA's anti-fraud unit, said in a recent telephone interview. David noted that other obscure areas of the Internet, such as the .tk domain associated with the South Pacific territory of Tokelau, have been used by opportunistic hackers.

"It's all about business," he said.

David and others say scammers began to move to .su after the administrators of Russia's .ru space toughened their rules back in late 2011.

Group-IB, which runs one of Russia's two official Internet watchdogs, says that the number of malicious websites hosted across the Soviet Union's old domain doubled in 2011 and doubled again in 2012, surpassing even the vast number of renegade sites on .ru and its newer Cyrillic-language counterpart.

The Soviet domain has "lots of problems," Group-IB's Andrei Komarov said in a phone interview. "In my opinion more than half of cybercriminals in Russia and former USSR use it."

The most notorious site was Exposed.su, which purportedly published credit records belonging to President Barack Obama's wife, Michelle, Republican presidential challengers Mitt Romney and Donald Trump,

and celebrities including Britney Spears, Jay Z, Beyonce and Tiger Woods. The site is now defunct.

Other Soviet sites are used to control botnets—the name given to the networks of hijacked computers used by criminals to empty bank accounts, crank out spam, or launch attacks against rival websites.

Employees of Moscow's Group-IB, which is responsible for one of Russia's two official Internet watchdogs, work in their laboratory in Moscow, Russia on Thursday, May 30, 2013. Figures supplied by Group-IB suggest that the number of malicious websites hosted across the Soviet Union's old domain doubled in 2011 and doubled again in 2012, surpassing even the vast number of renegade sites on .ru and its newer Cyrillic-language counterpart. (AP Photo/Alexander Zemlianichenko)

Internet hosting companies generally eliminate such sites as soon as

they're identified. But Swiss security researcher Roman Huessy, whose abuse.ch blog tracks botnet control sites, said hackers based in Soviet cyberspace can operate with impunity for months at a time.

Asked for examples, he rattled off a series of sites actively involved in ransacking bank accounts or holding hard drives hostage in return for ransom—brazenly working in the online equivalent of broad daylight.

"I can continue posting this list for ages," he said via Skype.

The history of .su goes back to the early days of the Internet, when its architects were creating the universe of country code suffixes meant to mark out a website's nationality. Each code—like .fr for France or .ca for Canada—was meant to correspond to a country.

Some Cold War-era domain names—such as .yu for Yugoslavia or .dd for East Germany—evaporated after the countries behind them disappeared. But the .su domain survived the dissolution of the Soviet Union in 1991 and the creation of a .ru domain in 1994, resisting repeated attempts to wipe it from the Web because, unlike other defunct domains, those behind .su refused to pull the plug—on both commercial and patriotic grounds.

With more than 120,000 domains currently registered, mothballing .su now would be a messy operation.

"It's like blocking .com or .org," said Komarov. "Lots of legitimate domains are registered there."

Among them are stalin.su, which eulogizes the Soviet dictator and the English-language chronicle.su, an absurdist parody site.

But experts say many are fraudulent, and even the organization behind

.su accepts it has a problem on its hands.

"We realize it's a threat for our image," said Sergei Ovcharenko, whose Moscow-based nonprofit Foundation for Internet Development took responsibility for .su in 2007.

Ovcharenko insisted that only a small number of .su sites are malicious, although he acknowledged that criminal sites can stay online for extremely long periods of time. He said his hands were tied by weak Russian legislation and outdated terms of service. But he promised that stricter rules are on their way after months of legal leg work.

"We are almost there," he said. "This summer, we'll be rolling out our new policy."

Meanwhile .su has become an increasingly notorious corner of the Internet, an online echo of the evil empire moniker assigned to the Soviet Union by U.S. President Ronald Reagan 30 years ago.

David, the RSA manager, said the emergence of a Communist relic as a 21st century security threat was a bizarre blast from the past.

"I thought that the Berlin Wall and my grandma's borscht are the only remnants of the Soviet Union," he said. "I was wrong."

More information: Group-IB: www.group-ib.com

Roman Huessy's website: www.abuse.ch

RSA: uk.emc.com/domains/rsa/index.htm

Foundation for Internet Development: www.fid.ru/english