# Researcher: Tools Will Help Personalize ID Theft by 2010

April 20 2007

A well-known security expert demonstrates a framework at the CanSecWest conference that makes it easier for criminals to steal identifying data.

Hackers with scrounged-up data ask the same question as dogs who've caught the school bus: What do we do with it now?

Roelof Temmingh has the answer, at least for rogue hackers, in the form of a framework that makes identity theft a much easier proposition. The framework, which is in the early stages of development, is called Evolution. Temmingh, a security expert who's authored well-known security testing applications such as Wikto and CrowBar , demonstrated Evolution during his opening presentation here at the CanSecWest security conference on April 18.

Evolution works by feeding on disparate identifying data such as name, e-mail address, company, word or phrase, and Web site - or the hacker's version of that, which would translate to IP address, virtual hosts, Netblocks/AS routes, affiliations (with social sites such as LinkedIn, MySpace, Facebook, and so on), forward and reverse DNS-MX/NS records, Whois records/rWhois and referring registrars, Google, and microformats including, for example, vCards.

The framework's genius lies in transforming one type of information to another. Evolution can transform a domain into an e-mail address or telephone number, or both (through the Whois domain name lookup

service), to related DNS names, to IPs, to a Web site, to e-mail addresses (again, via Whois), to telephone numbers, to geographic locations, to alternative e-mail addresses, to related telephone numbers, to co-hosted sites with the same IP, and so on.

The idea of using transforms to unearth hidden data builds on the logic that if A points to B points to C, and X points to Y points to C, then A points to X, Temmingh said. Transforms call on Java entities including affiliationEntity.java, DNSNameEntity.java, DocumentEntity.java, DomainEntity.java, EmailAddressEntity.java, and so on.

Evolution now contains 26 transforms and "is growing steadily," Temmingh said. An example of a transform that can move one type of information to another: PersonToEmailPhoneSiteGoogleBlog.java.

So what does that mean? The transforms are part of the answer to, "Who can do anything with a fill-in-the-blank?" Who can do anything with an e-mail address or a Social Security number, for example. Given a SSN and an entity with which to transform it, an identity thief or other criminal could do much, Temmingh said.

For example, with domain and e-mail data, a criminal can spoof e-mail to make it look as if it were coming from an internal source within a company. Making it look like an "accidental" cc, the crook could e-mail employees - or, less subtly, a business such as Bloomberg's - stating that the CEO has resigned, that the company is insolvent, that the recipient should hasten to sell his or her shares, and so on. Or a criminal could register a site in the name of the holding company's director and mirror a porn site to get it populated. Or spoof e-mail from a techie at a sister company to employees at a target company, mentioning a lamentable "discovery." Or spoof an SMS from a mobile phone to a high-profile investor about corruption in the company.

Next, sit back and watch share price drop. Buy low and sell high: the classic pump-and-dump scheme.

"It's kid's stuff, and it's easy to spot," Temmingh said. "Timing, however, is everything." If a criminal can do it at the right time, say, during a merger between two companies, the crime is likely to be successful, he said. "The only thing you need is to create doubt in the minds of other people."

To enable crimes such as these, a tool such as Evolution would come in handy. It returns hotlinked results in list form or in a spider diagram that shows each transform operation done on a given datum and where that transform leads. The question is, what does Temmingh intend to do with this potentially nefarious framework?

In fact, Evolution can do much on behalf of conventional security, he said. It can be used for standard footprinting (DNS, IPs and domains, for example), for identifying phishing sites or for finding partner alliances with weaker security postures.

On the other hand, it can also be used to identify targets for social engineering and client-side attacks, for finding war-dialing ranges, to find alternative e-mail addresses for content attacks, or to understand business drivers of specific organizations along with their sensitivities. For example, a socially engineered attack benefits greatly by having convincing backup data on hand, including knowing what the target's phone number or alternative e-mail addresses are.

This all demonstrates what Temmingh said is the scary side of Web 2.0. "Web 2.0 contains great technology, but little is known about the security implications when that technology is actually used," he said.

"Real criminals don't write buffer overflows," he said. "They follow the

route of least resistance."

Mainstream criminals tend to lag behind technological advance, he said. For example, phishing attacks were known about as far back as 1995. The question is, what will be on criminals' minds in 2010? Temmingh believes that the Internet's darker elements will be using tools "something close to" what he's demonstrated in Evolution: a framework that can execute personalized identity theft with scraps of information.

"[Criminals] will be able to have tools to merge this information together to manipulate outcome of certain events," Temmingh said.

If the examples given aren't scary enough, here are more that he described: Who at the NSA uses Gmail? Which NASA employees are using MySpace? Which people in Kabul are using Skype? In which countries do marines have bases? What are the names and e-mail addresses of single, young women in my neighborhood who are straight - or not?

Better yet, post a fake help wanted ad, Temmingh suggested: "Looking for a nuclear scientist/engineer with experience in uranium enrichment and military background. Earn top dollar. 401k plan, dental coverage, 25 days leave. Flex time."

After applicants send in their life stories on their resumes, go ahead and create an identity for them. Create an e-mail address with their name, post responses on blogs, join affiliation sites.

Thus criminals can concoct entire legions of half- (or more) fake but credible (online) people with whom they can do mischief, Temmingh said - another illustration of how, while the security implications of Web 2.0 have largely been overlooked, criminals will likely pick up on them in the near future.