Update on campaign targeting security researchers

blog.google/threat-analysis-group/update-campaign-targeting-security-researchers/

Adam Weidemann

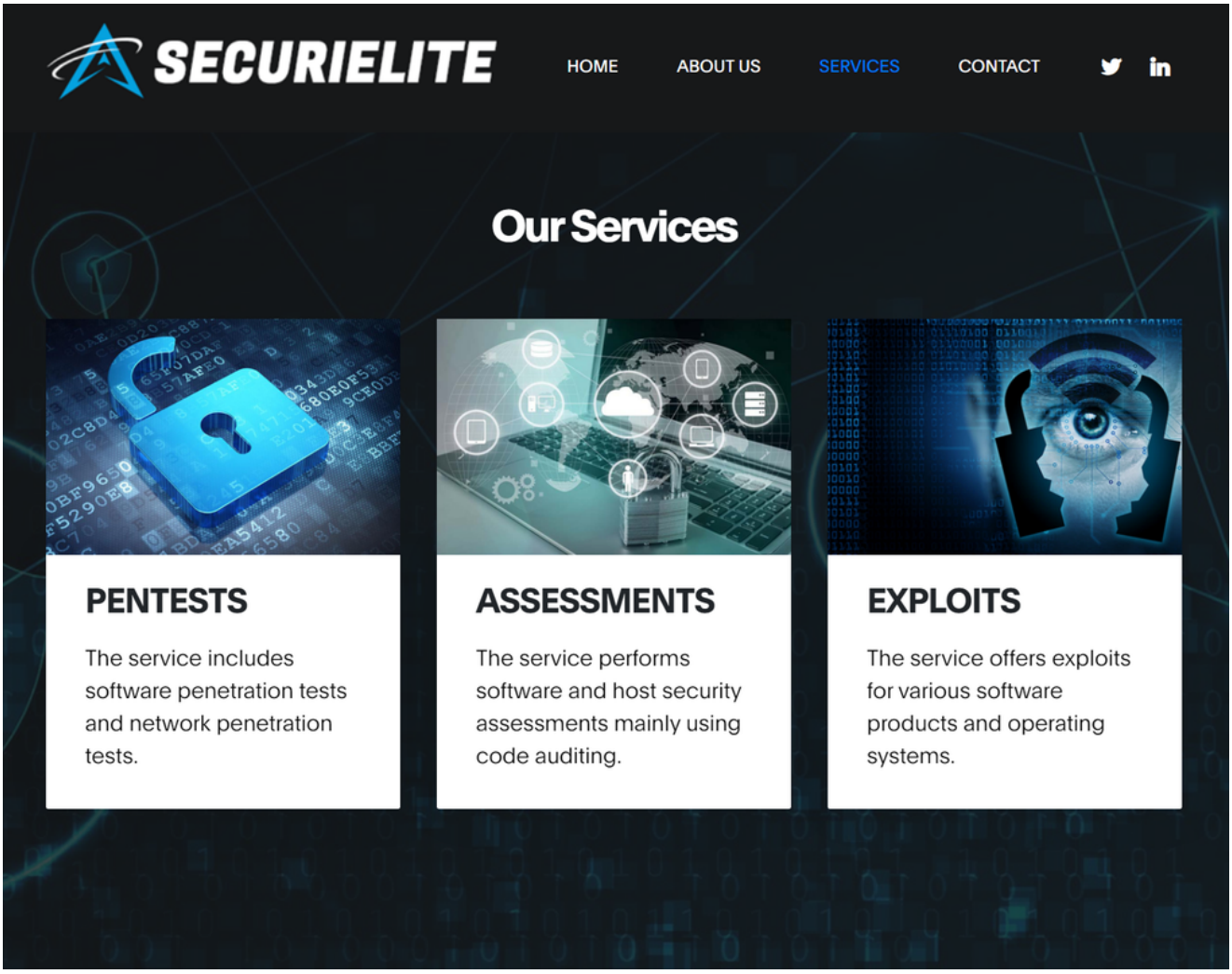
March 31, 2021

Threat Analysis Group

In January, the Threat Analysis Group documented a hacking campaign, which we were able to attribute to a North Korean government-backed entity, targeting security researchers. On March 17th, the same actors behind those attacks set up a new website with associated

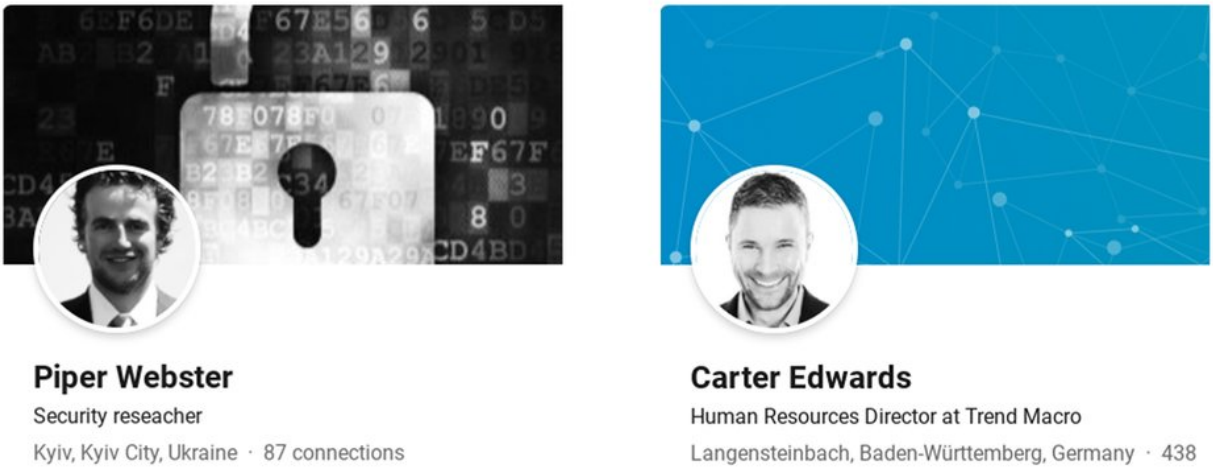
social media profiles for a fake company called “SecuriElite.”

The new website claims the company is an offensive security company located in Turkey that offers pentests, software security assessments and exploits. Like previous websites we’ve seen set up by this actor, this website has a link to their PGP public key at the bottom of the page. In January, targeted researchers reported that the PGP key hosted on the attacker’s blog acted as the lure to visit the site where a browser exploit was waiting to be triggered.



SecuriElite website

The attacker’s latest batch of social media profiles continue the trend of posing as fellow security researchers interested in exploitation and offensive security. On LinkedIn, we identified two accounts impersonating recruiters for antivirus and security companies. We have reported all identified social media profiles to the platforms to allow them to take appropriate action.



Actor controlled LinkedIn profiles

Actor controlled Twitter profiles

Tweet from SecuriElite announcing new company

At this time, we have not observed the new attacker website serve malicious content, but we have added it to Google Safebrowsing as a precaution.

Following our January blog post, security researchers successfully identified these actors using an Internet Explorer 0-day. Based on their activity, we continue to believe that these actors are dangerous, and likely have more 0-days. We encourage anyone who discovers a

Chrome vulnerability to report that activity through the Chrome Vulnerabilities Rewards Program submission process.

Actor controlled sites and accounts

Fake Security Company Website:

www.securielite[.]com

Twitter Profiles:

- https://twitter.com/alexjoe9983
- https://twitter.com/BenH3mmings
- https://twitter.com/chape2002
- https://twitter.com/julia0235
- https://twitter.com/lookworld0821
- https://twitter.com/osm4nd
- https://twitter.com/seb_lazar
- https://twitter.com/securielite

LinkedIn Profiles:

- SecuriElite - https://www.linkedin.com/company/securielite/
- Carter Edwards, HR Director @ Trend Macro - https://www.linkedin.com/in/carter-edwards-a99138204/
- Colton Perry, Security Researcher - https://www.linkedin.com/in/colton-perry-6a8059204/
- Evely Burton, Technical Recruiter @ Malwarebytes - https://www.linkedin.com/in/evely-burton-204b29207/
- Osman Demir, CEO @ SecuriElite - https://www.linkedin.com/in/osman-demir-307520209/
- Piper Webster, Security Researcher - https://www.linkedin.com/in/piper-webster-192676203/
- Sebastian Lazarescue, Security Researcher @ SecuriElite - https://www.linkedin.com/in/sebastian-lazarescue-456840209/

Email:

- contact@securielite.com
- osman@securielite.com
- submit@securielite.com

Attacker Owned Domains:

- bestwing[.]org
- codebiogblog[.]com
- coldpacific[.]com
- cutesaucepuppy[.]com
- devguardmap[.]org
- hireproplus[.]com
- hotelboard[.]org
- mediterraneanroom[.]org
- redeastbay[.]com
- regclassboard[.]com
- securielite[.]com
- spotchannel02[.]com
- wileprefgurad[.]net

POSTED IN:

Threat Analysis Group