Hackování RUAG. Švýcarský CERT odhalil podrobnosti o útoku

Vložil/a Cybersecurity H... [1], 24 Květen, 2016 - 17:11

- Exploit [2]
- Hacked Gallery [3]
- Hacking [4]
- Hacking method [5]
- Security [6]
- Top Secret [7]

V květnu se veřejnost dozvěděla o kyberbezpečnostním útoku na hlavního švýcarského vojenského dodavatele. RUAG popíral zprvu všechna obvinění z úniku citlivých dat. Dnes švýcarský CERT zveřejnil podrobnou zprávu o útoku, vysvětluje, jak se to stalo a kdy.

Tato zpráva je k dispozici zde, kde si ji může každý stáhnout a přečíst.

Podle zjištění poskytnutých výzkumnými pracovníky narušení bezpečnosti proběhlo v září 2014, ale bylo objeveno až v lednu 2016. Útočníci měli přístup k síti RUAG déle než jeden rok a zajisté ukradli spoustu důvěrných informací.

Souhrnná zpráva říká: "Útočníci ukázali velkou trpělivost během infiltrace a laterální pohyb. Napadli jen oběti, které měli zájem o provádění různých opatření, jako je například cílový IP seznam a rozsáhlé otisky prstů před a po počáteční nákaze. Poté, co se dostali do sítě, laterálně se posunuli pomocí infikování dalších zařízení a dosáhnutí vyšších oprávnění ".

Nebylo možné, aby výzkumníci zjistili, jak útočníci narušili síť, protože soubory protokolu z doby průniku byly dlouho smazány a mnoho počítačů bylo přeinstalováno nebo vyměněno.

Útočníci byli opatrní při odcizení informací. Maskovali exfiltraci dat v provozu HTTP a používali port 80 / TCP pro připojení k C&C serverům.

By Cybersecurity Help [8] =)

URL článku: https://security-portal.cz/node/3757

Odkazy:
[1] https://security-portal.cz/users/cybersecurity-help-sro
[2] https://security-portal.cz/category/tagy/exploit
[3] https://security-portal.cz/category/tagy/hacked-gallery
[4] https://security-portal.cz/category/tagy/hacking
[5] https://security-portal.cz/category/tagy/hacking-method
[6] https://security-portal.cz/category/tagy/security
[7] https://security-portal.cz/category/tagy/top-secret
[8] https://www.cybersecurity-help.cz/cz/blog/124.html