GAMAREDON GROUP

AXIAL

A SURVEY ON GAMAREDON GROUP: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

Gamaredon Group is a threat group that has been active since at least 2013 and has targeted individuals likely involved in the Ukrainian government. The name Gamaredon Group comes from a misspelling of the word "Armageddon", which was detected in the adversary's early campaigns. The Gamaredon Group has relied heavily on off-the-shelf tools.

II. TARGET SECTORS

Defense, Government, Law enforcement, NGOs and diplomats and journalists.

III. METHODS USED

Generally, they use phising mails with a malware attachment.

IV. ENGAGEMENTS

- Apr 2019, The discovered attack appears to be designed to lure military personnel: it leverages a legit document of the “State of the Armed Forces of Ukraine” dated back in the 2nd April 2019.
- May 2019, The Gamaredon attacks against Ukraine doesn’t seem to have stopped. After a month since our last report, we spotted a new suspicious email potentially linked to the Gamaredon group.
- Jul 2019, EvilGnome: Rare Malware Spying on Linux Desktop Users.
- Oct 2019, Lure documents observed appear to target Ukrainian entities such as diplomats, government employees, military officials, and more.
- Dec 2019, Gamaredon APT Improves Toolset to Target Ukraine Government, Military.
- Mar 2020, Moving into March 2020, countries worldwide are still struggling to manage the spread of the viral disease now known as COVID-19. In cyberspace, threat actors are using the topic of COVID-19 to their advantage with numerous examples of malicious activity using COVID-19 as lure documents in phishing campaigns.

AX1AL

V. IOC

C&C

1. **Bambinos[.]bounceme[.]net**
2. **bbtt[.]site**
3. **bbtt[.]space**
4. **harpa[.]siteharpa[.]space**
5. **harpa[.]website**

MD5

1. **17161e0ab3907f637c2202a384de67fca49171c79b1b24db7c78a4680637e3d5**
2. **29367502e16bf1e2b788705014d0142d8bcb7fcc6a47d56fb82d7e333454e923**
3. **315e297ac510f3f2a60176f9c12fcf92681bbad758135767ba805cdea830b9ee**
4. **3e6166a6961bc7c23d316ea9bca87d8287a4044865c3e73064054e805ef5ca1a**
5. **3f40d4a0d0fe1eea58fa1c71308431b5c2ce6e381cacc7291e501f4eed57bfd2**

VI. REFERENCES

- https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution/
- https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/
- https://blog.trendmicro.com/trendlabs-security-intelligence/gamaredon-apt-group-use-covid-19-lure-in-campaigns/
- https://attack.mitre.org/groups/G0047/