APT-C-53 Gamaredon

Recently, 360 Security Brain has detected more frequent network attacks related to the APT-C-53 (Gamaredon) organization, and found that the organization began to release the open source DDoS Trojan program " LOIC " to carry out DDoS attacks.

in the rightDuring the monitoring of APT-C-53 (Gamaredon) network attacks , we found multiple attack chains: phishing emails, file remote template injection execution, S FX self-extracting program execution of malicious scripts, Wiper malware delivery, And registry write load schedule task execution and so on.

Through continuous mining, we have captured the network attack activities of multiple APT-C-53 (Gamaredon) organizations , and found related samples and C 2 servers . During the monitoring process of this batch of C 2 servers , We found that multiple C2 servers distributed an open source D Dos Trojan program L OIC compiled by .net from March 4th to 5th, 2022 .

The C& C domain name addresses involved in the DD o S attack task delivery :

decree.maizuko.**

caciques.gloritapa.**

delicate.maizuko.**

jealousy.jump.artisola.**

dense.gitrostan.**

decision.lotorgas.**

decency.maizuko.**

junior.jacket.artisola.**

defective88.maizuko.**

deception.lotorgas.**

destination.delight.coffiti.**

cachinate.gloritapa.**

January.josie.artisola.**

defective19.maizuko.**

deception.lotorgas.**

destination.delight.coffiti.**

DDoS program sample file information:

MD 5 5486BCE58C5D30C7B3F940079C33B95F

CompileTimestamp 2022/3/4 21:53

File Size _ _ 156.16K

The attacker hard-coded the IP address and port into the configuration, specifying the IP address for a DDoS attack .

```
namespace PS5
{
    // Token: 0x0200000C RID: 12
    internal static class Program
    {
        // Token: 0x06000064 RID: 100 RVA: 0x0000AB38 File Offset: 0x00008D38
        [STAThread]
        private static void Main(string[] cmdLine)
        {
            bool hive = true;
            bool hide = true;
            string ircserver = "70.34.203.4";
            string ircport = "6667";
            string ircchannel = "#loic";
            int num = 0;
            foreach (string text in cmdLine)
            {
                if (text.ToLowerInvariant() == "/hidden")
                {
                    hide = true;
                }
                if (text.ToLowerInvariant() == "/hivemind")
                {
                    hive = true;
                }
                num++;
            }
            Application.SetCompatibleTextRenderingDefault(false);
            Application.Run(new frmMain(hive, hide, ircserver, ircport, ircchannel));
        }
```

DDoS software is run by VBS script and Powershell script, and L OIC is the open source software of Git Hub . (https://github.com/NewEraCracker/LOIC)

Summarize This time , we observed the recent D DoS attack intention of APT-C-53 (Gamaredon) organization through the vision of 360 Security Brain for the first time . The distribution of the L OIC Trojan may be the prelude to a new round of D DoS attacks .

Appendix IOC

5486BCE58C5D30C7B3F940079C33B95F

e6655dedab03f67272542ed736c0d44d

be3b5e1525d8ab5af3a54b938c22df24

534bb9ccf8a6d8742ba6f68a67d2e2f2

d4683582d8bbaee8ffa959637234486e

9f3791d404f8710390fffa95aaa73b20

6151a1019b01ea4d9f4b31cd922fa5a4

5403b82909a1bf2902dbf916f3d3adee

daa93dd8aa1843d81179ac2375bb7a57

a4cf1a8c599a9f2de144075eba6de9d9

a0ec350d97c4bb602ca62f5dd5c1d7c7

6e935cf5bbfc7bbca15fba36573ba271

f37eb0915783d6a698eb2719885a7afe

558f254e4bc2410cd39a3cff735b520d

b09a504ebd900c40c4ca1ee66ab874a1

e4d2d113bc8eaa47cd2b0417c28b4232

c33531d82af89d1753e03438c7fabb75

52927e7034ef1c5ced76397c7a9451fc

5942d41337ee474c4f5ba2f94471e313

360 Advanced Threat Institute

360 Advanced Threat Research Institute is the core capability support department of 360 Government and Enterprise Security Group. It is composed of 360 senior security experts and focuses on the discovery, defense, disposal and research of advanced threats. It has taken the lead in capturing double kills, double stars and nightmares on a global scale. Formula and many other well-known 0-day in-the-field attacks, exclusively disclosed the advanced actions of several national-level APT organizations, and won wide recognition both inside and outside the industry, providing strong support for 360 to ensure national network security.