Researchers Disclose Undocumented Chinese Malware Used in Recent Attacks

thehackernews.com/2021/01/researchers-disclose-undocumented.html

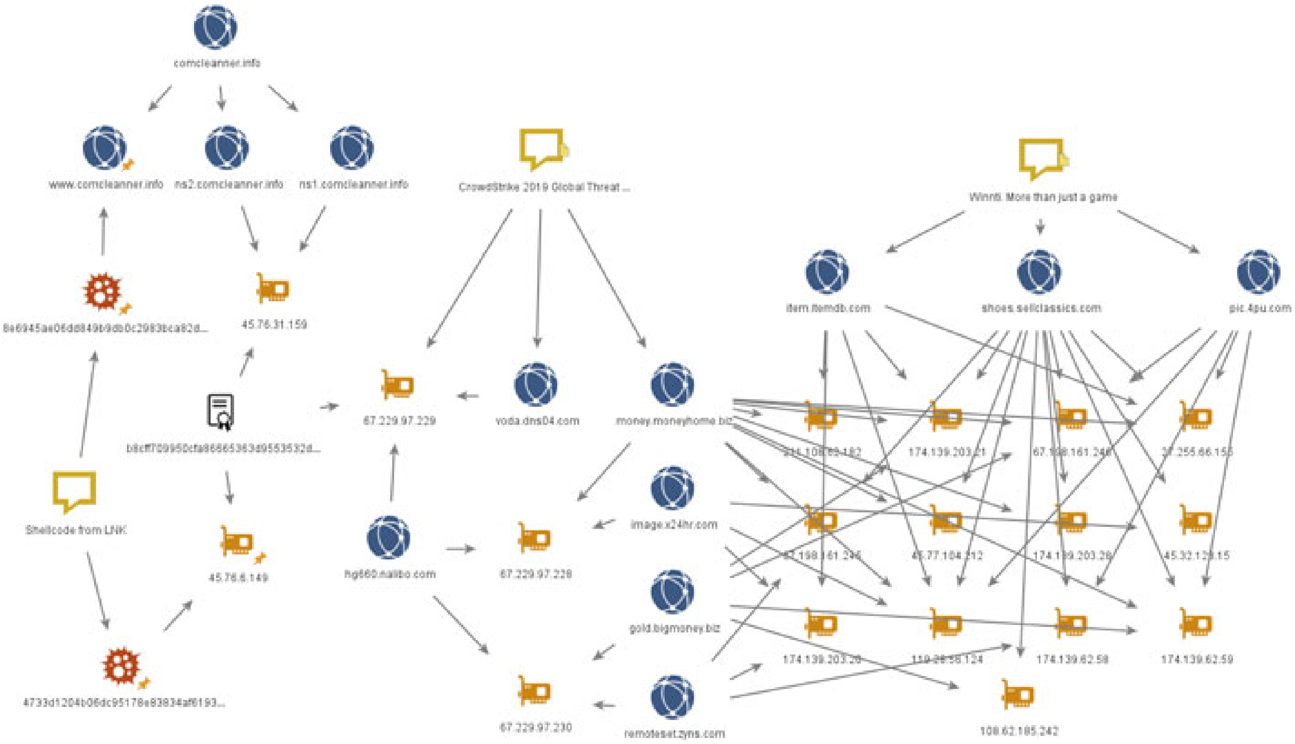
January 15, 2021

Cybersecurity researchers have disclosed a series of attacks by a threat actor of Chinese origin that has targeted organizations in Russia and Hong Kong with malware — including a previously undocumented backdoor.

Attributing the campaign to Winnti (or APT41), Positive Technologies dated the first attack to May 12, 2020, when the APT used LNK shortcuts to extract and run the malware payload. A second attack detected on May 30 used a malicious RAR archive file consisting of shortcuts to two bait PDF documents that purported to be a curriculum vitae and an IELTS certificate.

The shortcuts themselves contain links to pages hosted on Zeplin, a legitimate collaboration tool for designers and developers that are used to fetch the final-stage malware that, in turn, includes a shellcode loader ("svchast.exe") and a backdoor called Crosswalk ("3t54dE3r.tmp").

Crosswalk, first documented by FireEye in 2017, is a bare-bones modular backdoor capable of carrying out system reconnaissance and receiving additional modules from an attacker-controlled server as shellcode.



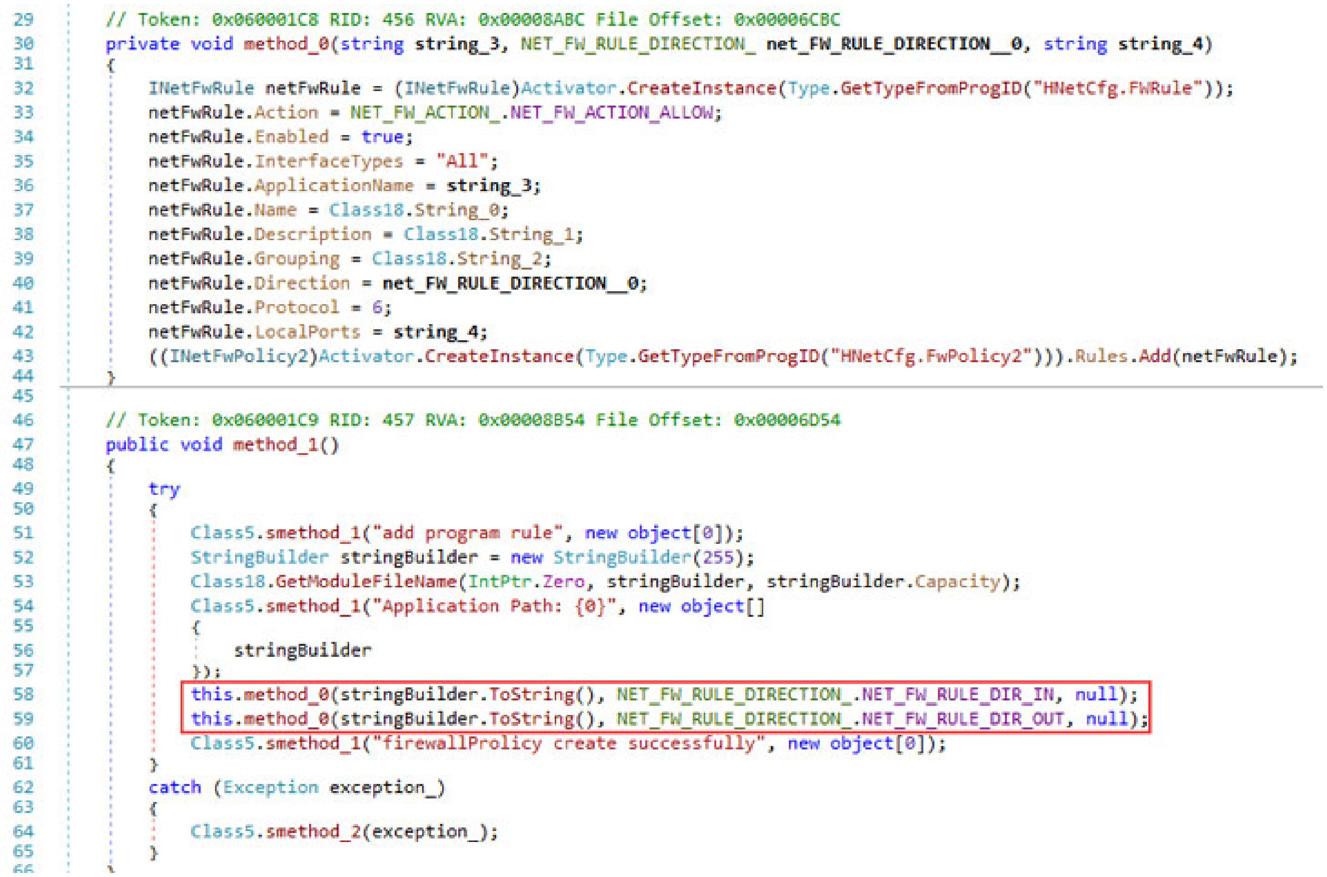
While this modus operandi shares similarities with that of the Korean threat group Higaisa — which was found exploiting LNK files attached in an email to launch attacks on unsuspecting victims in 2020 — the researchers said the use of Crosswalk suggests the involvement of Winnti.

This is also supported by the fact that the network infrastructure of the samples overlaps with previously known APT41 infrastructure, with some of the domains traced back to Winnti attacks on the online video game industry in 2013.

The new wave of attacks is no different. Notably, among the targets include Battlestate Games, a Unity3D game developer from St. Petersburg.

Furthermore, the researchers found additional attack samples in the form of RAR files that contained Cobalt Strike Beacon as the payload, with the hackers in one case referencing the U.S. protests related to the death of George Floyd last year as a lure.

In another instance, Compromised certificates belonging to a Taiwanese company called Zealot Digital were abused to strike organizations in Hong Kong with Crosswalk and Metasploit injectors, as well as ShadowPad, Paranoid PlugX, and a new .NET backdoor called FunnySwitch.



```
// Token: 0x060001C8 RID: 456 RVA: 0x00008ABC File Offset: 0x00006CBC
private void method_0(string string_3, NET_FW_RULE_DIRECTION_ net_FW_RULE_DIRECTION__0, string string_4)
{
    INetFwRule netFwRule = (INetFwRule)Activator.CreateInstance(Type.GetTypeFromProgID("HNetCfg.FWRule"));
    netFwRule.Action = NET_FW_ACTION_.NET_FW_ACTION_ALLOW;
    netFwRule.Enabled = true;
    netFwRule.InterfaceTypes = "All";
    netFwRule.ApplicationName = string_3;
    netFwRule.Name = Class18.String_0;
    netFwRule.Description = Class18.String_1;
    netFwRule.Grouping = Class18.String_2;
    netFwRule.Direction = net_FW_RULE_DIRECTION__0;
    netFwRule.Protocol = 6;
    netFwRule.LocalPorts = string_4;
    ((INetFwPolicy2)Activator.CreateInstance(Type.GetTypeFromProgID("HNetCfg.FwPolicy2"))).Rules.Add(netFwRule);
}

// Token: 0x060001C9 RID: 457 RVA: 0x00008B54 File Offset: 0x00006D54
public void method_1()
{
    try
    {
        Class5.smethod_1("add program rule", new object[0]);
        StringBuilder stringBuilder = new StringBuilder(255);
        Class18.GetModuleFileName(IntPtr.Zero, stringBuilder, stringBuilder.Capacity);
        Class5.smethod_1("Application Path: {0}", new object[]
        {
            stringBuilder
        });
        this.method_0(stringBuilder.ToString(), NET_FW_RULE_DIRECTION_.NET_FW_RULE_DIR_IN, null);
        this.method_0(stringBuilder.ToString(), NET_FW_RULE_DIRECTION_.NET_FW_RULE_DIR_OUT, null);
        Class5.smethod_1("firewallProlicy create successfully", new object[0]);
    }
    catch (Exception exception_)
    {
        Class5.smethod_2(exception_);
    }
}
```

The backdoor, which appears to be still under development, is capable of collecting system information and running arbitrary JScript code. It also shares a number of common features with Crosswalk, leading the researchers to believe that they were written by the same developers.

Previously, Paranoid PlugX had been linked to attacks on companies in the video games industry in 2017. Thus, the deployment of the malware via Winnti's network infrastructure adds credence to the "relationship" between the two groups.

"Winnti continues to pursue game developers and publishers in Russia and elsewhere," the researchers concluded. "Small studios tend to neglect information security, making them a tempting target. Attacks on software developers are especially dangerous for the risk they pose to end users, as already happened in the well-known cases of CCleaner and ASUS."

SHARE □ □ □ □ □
SHARE □
Cyber Attack, Malware, Phishing