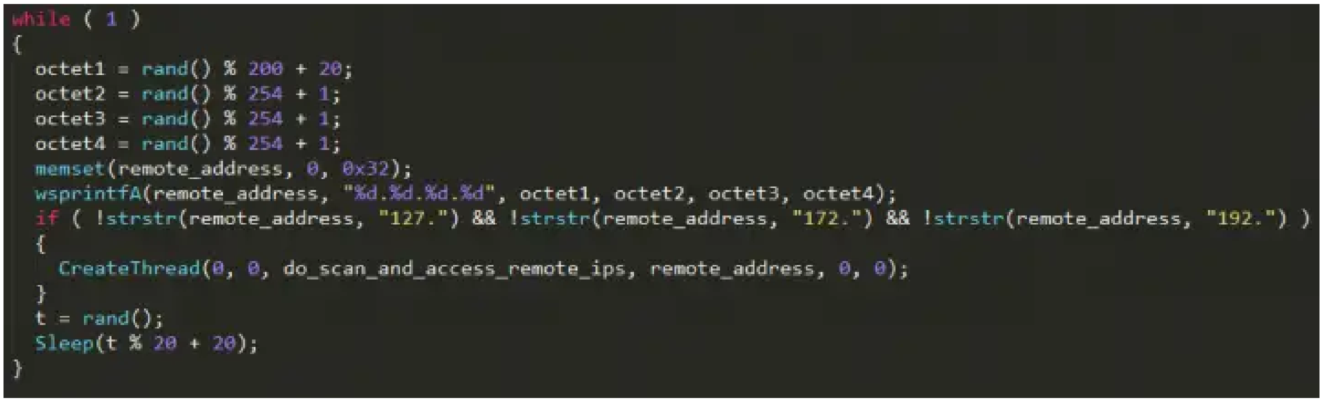
Nemty Ransomware Expands Its Reach, Also Delivered by Trik Botnet

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nemty-ransomware-trik-botnet



```
while ( 1 )
{
  octet1 = rand() % 200 + 20;
  octet2 = rand() % 254 + 1;
  octet3 = rand() % 254 + 1;
  octet4 = rand() % 254 + 1;
  memset(remote_address, 0, 0x32);
  wsprintfA(remote_address, "%d.%d.%d.%d", octet1, octet2, octet3, octet4);
  if ( !strstr(remote_address, "127.") && !strstr(remote_address, "172.") && !strstr(remote_address, "192.") )
  {
    CreateThread(0, 0, do_scan_and_access_remote_ips, remote_address, 0, 0);
  }
  t = rand();
  Sleep(t % 20 + 20);
}
```

Figure 4. Trik’s SMB component generates random remote IP addresses to connect to

From analysing the malware’s code, we can see that it skips the routine if the created IP address is a local one (Figure 4). The malware can infect public IP addresses with port 139 open that are using any of the common administrator usernames and passwords on its list.

Usernames: Administrator, administrator, Admin, admin

Passwords: 123, 1234, 12345, 123456, 1234567, 12345678, 123456789, 1234567890, 123123, 12321, 123321, 123abc, 123qwe, 123asd, 1234abcd, 1234qwer, 1q2w3e, a1b2c3, administrator, Administrator, admin, Admin, admin123, Admin123, admin12345, Admin12345, administrator123, Ad ministrator123, nimda, qwewq, qweewq, qwerty, qweasd, asdsa, asddsa, asdzxc, asdfgh, qweasdzxc, q1w2e3, qazwsx, qazwsxedc, zxcxz, zxccxz, zxcvb, zxcvbn, passwd, password, Password, login, Login, pass, mypass, mypassword, adminadmin, root, rootroot, test, testtest, temp, temptemp, foofoo, foobar, default, password1, password12, password123, admin1, admin12, admin123, pass1, pass12, pass123, root123, abc123, abcde, abcabc, qwe123, test123, temp123, sample, example, internet, Internet

If access is granted, the malware uses the SMB protocol to copy itself to the remote machine. It then uses the Windows Service Control Manager to start the SMB component's process on the remote machine. The sample running on the remote machine also checks for the presence of winsvcs.txt, which again determines whether or not Nemty is downloaded and executed.

About the Author

Nguyen Hoang Giang

Senior Threat Analysis Engineer

Hoang Giang is a member of the Threat Engineering team in Symantec's Security Technology and Response (STAR) division. He analyzes and creates protection for various threats and monitors for botnets and APT attacks.

About the Author

Eduardo Altares

Senior Threat Analysis Engineer

Eduardo is a member of Symantec's Security Technology and Response (STAR) team who are focused on providing round-the-clock protection against current and future cyber threats.

About the Author

Muhammad Hasib Latif

Senior Threat Analysis Engineer

Hasib is a member of Symantec’s Security Technology and Response (STAR) team who are focused on providing round-the-clock protection against current and future cyber threats.