Plantilla para la presentación de ponencias

EVOLUCIÓN DE LOS SERVICIOS DE ANONIMIZACIÓN EMPLEADOS PARA EL ACCESO INICIAL EN INTRUSIONES: EL CASO DE LOS PROXYS RESIDENCIALES[1]

Enrique DE LA HOZ[2], Pablo ROSADO[2]

[1] *Universidad de Alcalá* [2]*Telefónica España*

enrique.delahoz@uah.es, pablo.rosadogonzalez@telefonica.com

Línea temática: **Seguridad y Privacidad.**

Resumen:
En los últimos años, se ha observado un aumento del número e impacto de las acciones maliciosas contra empresas y organizaciones, principalmente relacionado con las amenazas de tipo ransomware pero también por la extensión de la actividad de otras amenazas avanzadas. En paralelo, y en parte gracias a la creciente visibilidad que se disponer gracias a la compartición de información de ciberamenazas, se observa también una mayor sofisticación de las capacidades de los actores maliciosos. En este trabajo, nos centramos en la evolución de la infraestructura empleada por estos actores y, en particular, en la tipología y servicios empleados como orígenes de los accesos remotos a los sistemas, principalmente relacionados, aunque no exclusivamente, con el empleo de técnicas como 'Valid Accounts' (T1078) y 'External Remote Services' (T1133). Nuestra hipótesis de trabajo es que los atacantes, a lo largo de estos años, han evolucionado de intentar ocultar el verdadero origen de la actividad maliciosa, mediante el empleo de redes de anonimización como Tor y servicios de VPN, a intentar mimetizarse con la actividad común en un sistema, aprovechando servicios existentes o procurándose una infraestructura que les permitiera disponer de orígenes de su actividad similares a los de los usuarios legítimos del sistema. Si bien estos patrones de actividad no son nuevos y han sido documentados en el pasado asociados a APTs, en los últimos años grupos de un menor nivel de sofisticación han

[1] *En esta charla, no se mencionará ningún tipo de producto o servicio proporcionado por Telefónica España ni se hará referencia a ningún elemento comercial. La presentación, de ser aceptada, la realizaría Enrique de la Hoz, como miembro de la Universidad de Alcalá.*

aprovechado servicios legítimos, como los conocidos como proxys residenciales para vehicular esa actividad maliciosa. En esto servicio, usuarios, en muchas ocasiones sin ser conscientes de ello, cede la utilización de su conexión a internet para el enrutamiento de tráfico de otros usuarios. Gracias a esquemas de distribución que en ocasiones son poco claros, estos servicios han conseguido un número muy elevado de accesos, que en España se cifraría en varios millones según varios proveedores, que permite a los clientes de estos servicios enrutar el tráfico web que deseen seleccionando orígenes según proveedor de servicios de internet, o ubicación geográfica detallada. En este trabajo, presentamos las principales características de este tipo de servicios, explicaremos algunos escenarios de empleo en campañas reales y plantearemos los principales riesgos que pueden suponer para las organizaciones que forman parte de RedIRIS. Por último, realizaremos una presentación del grado de penetración de este tipo de herramientas en los accesos a Internet en España tanto residenciales como corporativos que es, en nuestro conocimiento, el primero de este tipo que se ha llevado a cabo.

Palabras claves:
Acceso inicial, anonimización, proxys residenciales.

Abstract:

In recent years, there has been an increase in both the number and the impact of malicious actions against companies and organizations, mainly related to ransomware-type threats, but also linked to the expansion of activities by other advanced threats. In parallel—and partly thanks to the growing visibility provided by cyber threat information sharing—there has been a marked increase in the sophistication of malicious actors' capabilities. This paper focuses on the evolution of the infrastructure employed by these actors, with particular attention to the typology and services used as sources of remote system access, primarily (though not exclusively) associated with techniques such as "Valid Accounts" (T1078) and "External Remote Services" (T1133).

Our working hypothesis is that attackers have shifted over the years from merely concealing the true origin of malicious activity—through anonymization networks like Tor and VPN services—to attempting to blend in with normal system activity. They do this by exploiting existing services or establishing an infrastructure that provides origins of activity closely resembling those of legitimate system users. While these activity patterns are not new and have been documented in the past in relation to APTs (Advanced Persistent Threats), in recent years, groups with a lower level of sophistication have taken advantage of legitimate services, such as so-called "residential proxies," to carry out malicious actions. In these services, users often unwittingly allow their internet connection to be used for routing other users' traffic. Thanks to occasionally obscure distribution schemes, these services have

amassed a very large number of access points—reaching several million in Spain, according to multiple providers—and permit their customers to route web traffic while selecting its origin by internet service provider or specific geographic location.

In this paper, we describe the main characteristics of these services, illustrate their use in actual campaigns and discuss the major risks they pose to organizations from RedIRIS. Finally, we present the degree to which these tools have penetrated both residential and corporate internet accesses in Spain, a study that, to our knowledge, is the first of its kind.

Keywords:
Anonymization, Initial Access, Residential Proxies